
青年科學叢書
方程式的整數解
蓋里馮德著
中國青年出版社

序

這本書是根據我1951年在莫斯科大學數學競賽會上宣讀過的方程式整數解的講演稿編寫的。 我利用這個機會，順便向我的學生戈羅博夫（Н. М. Коробов）講師致謝，他依照我講演稿的大綱，幫助我編寫了第一、第二兩節和第三節的一部分。

這本書對於高年級的中學生是不難了解的。

A. 蓋里馮德

目　　次

緒 言

數論基本上研究的是自然數列中數的算術性質，換句話說，就是正整數的算術性質，它是一門古老的數學。所謂數的解析理論中的一個中心問題，就是自然數列中質數分佈的問題。只能夠被自己和1除盡的任何大於1的正整數，叫做質數。自然數列中質數分佈的問題，在於研究當數值N很大時，小於N的質數的數目的變化規律。在這方面，第一個結果，我們可以在歐幾里得（公元前四世紀）的著作裏找到，即質數列是無限的證明。而在歐幾里得以後的第二個結果，是十九世紀後半期偉大的俄國數學家切貝雪夫（П. Л. Чебышев）得到的。數論的另外一個基本問題，就是關於用某種類型的整數和來表示整數的問題，例如用三個質數的和來表示一個奇數的問題。後面一個問題，就是哥特巴赫問題，是在不久以前，由數論的傑出代表、蘇聯數學家維諾格拉多夫（И. М. Виноградов）解決的。

請讀者注意，這本書講的也是數論中特別有趣味的一部分，即方程式的整數解。

求具有一個以上未知數的整數係數代數方程式的整數解，是數論中一個很困難的問題。許多古代最卓越的數學家都曾經研究過許多這樣的問題，例如希臘數學家畢達果拉斯（公元前六世紀），亞歷山大城的丟番圖（公元二-三世紀）以及

比較近代的最優秀數學家飛馬(十七世紀),歐拉(十八世紀),拉格朗奇(十八世紀)等等.不管若干代卓越數學家們怎樣努力,在這個領域中,仍然缺乏某種一般性的方法,能夠用來解決非常複雜的解析數論的問題,如像維諾格拉多夫的三角法的和那一類型的方法那樣.

求方程式整數解的問題,結局只解決了二元二次方程式的問題.我們注意,對於一元任意次方程式來說,這個問題並沒有多大用處,因為這個問題可以借助於有限個數目的試驗來解決. 對於高於二次的二元或多元方程式,不只是求一切整數解的問題,甚至於更簡單的,確定這樣的解是有限或無限多的問題都是極困難的.

求方程式的整數解不只具有理論的利益.這樣的方程式有時在物理學中也會遇到.

方程式整數解的理論利益是非常鉅大的,因為這些方程式和許多數論問題都有密切聯系. 除此以外,在這書裏敍述的這種方程式的初步理論,對於中學生、專科學校和高等師範教員,用來擴大數學的眼界也是可能有效的.

在這本書裏,我們敍述了方程式整數解在理論上得到的幾個主要結果. 書裏敍述的定理,在它的證明非常簡易的時候,我們就給與證明.

一 一元方程式

我們來研究一元一次方程式

$$a_1x+a_0=0. \tag{1}$$

設方程式的係數 a_1 和 a_0 是整數．很明白地，這個方程式的解

$$x=-\frac{a_0}{a_1},$$

只有在 a_0 能夠被 a_1 整除的時候，它才是整數． 由此可知，方程式(1)不是隨時都有整數解的；例如，這兩個方程式

$$3x-27=0 \text{ 和 } 5x+21=0$$

中，第一個具有整數解 $x=9$，而第二個就不可能有整數解。

在次數高於一的方程式中，我們也遇到同樣的情形：二次方程式

$$x^2+x-2=0$$

具有整數解 $x_1=1$， $x_2=-2$；方程式

$$x^2-4x+2=0$$

就不可能有整數解，因爲它的根 $x_{1,2}=2\pm\sqrt{2}$ 是無理數．

關於求出整數係數的 n 次方程式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0=0 \quad (n\geqslant 1) \qquad (2)$$

的整數根，這個問題很容易解決． 事實上，設 $x=\alpha$ 是這個方程式的整數根，那末

$$a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots\cdots+a_1\alpha+a_0=0,$$

$$a_0=-\alpha(a_n\alpha^{n-1}+a_{n-1}\alpha^{n-2}+\cdots\cdots+a_1).$$

從末了一個等式可以看出，a_0 能被 α 除盡；由此可知，方程式(2) 的每一個整數根都是這個方程式絕對項的因數． 要求出這個方程式的整數解，就應當從 a_0 的因數中去挑選，把挑選出的數代入方程式，方程式就會變成恆等式．例如，從方程式

$$x^{10}+x^7+2x^3+2=0$$

的絕對項分解出來的一切因數 1，-1，2 和 -2 中，只有 -1 是

這個方程式的根. 由此可知,這個方程式具有唯一的整數根 $x=-1$. 用同樣的方法,容易證明,方程式

$$x^6-x^5+3x^4+x^2-x+3=0$$

不可能有整數根.

求多元方程式的整數解是很有趣的.

二　二元一次方程式

我們來研究二元一次方程式

$$ax+by+c=0, \tag{3}$$

這兒 a 和 b 是零以外的整數,而 c 是任意的整數. 我們將認定係數 a 和 b 不具有 1 以外的公因數㊀. 事實上,如果這兩個係數有 1 以外的最大公因數 $d=(a,b)$,則等式

$$a=a_1d,\quad b=b_1d,$$

是正確的;而方程式(3)就具有這樣的形式

$$(a_1x+b_1y)d+c=0,$$

因而只有在 c 能被 d 整除的情況,它才能夠具有整數解. 這樣一來,在 $(a,b)=d\neq1$ 的情況下,方程式 (3) 的一切係數都應當能夠被 d 整除,並且用 d 除(3),使方程式成爲

$$a_1x+b_1y+c_1=0\qquad (c_1=\frac{c}{d}),$$

方程式的係數 a_1 和 b_1 就是互質數.

我們首先研究當 $c=0$ 時的情形. 將方程式(3)改寫成這樣:

㊀ 這樣的數 a 和 b 叫做互質數;我們用 (a,b) 來表示兩個數 a 和 b 的最大公因數,對於互質數就得 $(a,b)=1$.

$$ax+by=0, \qquad (3')$$

對於 x 解這個方程式,得:

$$x=-\frac{b}{a}y.$$

很明白地,當 y 被 a 除得盡的時候,在這種情形也只有在這種情形,x 才具有整數值. 但 a 的倍數的一切整數 y,可以表示成這樣

$$y=at,$$

這兒 t 可以取任何整數值($t=0,\pm1,\pm2,\cdots\cdots$). 將這個 y 的值代入上面的方程式,則

$$x=-\frac{b}{a}at=-bt,$$

於是我們得到包括方程式(3′)的一切整數解的公式:

$$x=-bt,\ y=at\ (t=0,\pm1,\pm2,\cdots\cdots).$$

現在我們進到 $c\neq0$ 的情形.

我們首先證明,要求方程式(3)的一切整數解,只須找出它的任何一組解就夠了,也就是求出這樣的整數 x_0, y_0,使得

$$ax_0+by_0+c=0.$$

〔定理 1〕 設 a 和 b 是互質數,$[x_0,y_0]$是方程式

$$ax+by+c=0 \qquad (3)$$

的某一組解㊀;則公式

$$x=x_0-bt,\ y=y_0+at, \qquad (4)$$

取 $t=0,\pm1,\pm2,\cdots\cdots$就給出方程式(3)的一切解.

〔證明〕 設 $[x,y]$是方程式(3)的任何一組解. 則從等式

㊀ 一對適合於方程式的整數 x 和 y,叫做一組解,而用$[x,y]$表示.

$$ax+by+c=0 \quad 和 \quad ax_0+by_0+c=0,$$

我們得：

$$ax-ax_0+by-by_0=0; \quad y-y_0=\frac{a(x_0-x)}{b}.$$

因為 $y-y_0$ 是整數，並且 a 和 b 是互質數，則 x_0-x 必須能夠被 b 整除，即 x_0-x 具有這樣的形式

$$x_0-x=bt,$$

這兒 t 是整數．於是

$$y-y_0=\frac{abt}{b}=at,$$

並且我們得：

$$x=x_0-bt, \quad y=y_0+at.$$

這樣一來，就證明了任何一組解 $[x,y]$ 具有形式(4)．還剩下來檢查一下，由公式(4)取整數 $t=t_1$，得出來的任何一對數 $[x_1,y_1]$ 都是方程式(3)的解．為了施行這樣的檢查，將數值

$$x_1=x_0-bt_1, \quad y_1=y_0+at_1$$

代入方程式(3)的左邊，

$$ax_1+by_1+c=ax_0-abt_1+by_0+abt_1+c$$
$$=ax_0+by_0+c,$$

但因為 $[x_0,y_0]$ 是一組解，所以 $ax_0+by_0+c=0$，由此可見

$$ax_1+by_1+c=0,$$

即 $[x_1,y_1]$ 是方程式(3)的一組解，這定理就完全證明了．

這樣一來，倘若知道了方程式

$$ax+by+c=0$$

的一組解，則其他的一切解可由算術級數求出來，這算術級數

的一般項具有這樣的形式

$$x=x_0-bt,\ y=y_0+at\quad (t=0,\pm1,\pm2,\cdots\cdots).$$

我們注意,在 $c=0$ 時,前面求得的解的公式

$$x=-bt,\quad y=at$$

可以從剛才得到的公式

$$x=x_0-bt,\ y=y_0+at$$

中去掉 $x_0=y_0=0$ 得出來 這是可以做到的,因爲數值 $x=0$, $y=0$ 總是方程式

$$ax+by=0$$

的一組解。

在 $c\neq0$ 的一般情況,怎樣求出方程式(3)的某一組解 $[x_0,y_0]$ 呢? 我們先來舉一個例子.

設已知方程式是

$$127x-52y+1=0.$$

我們要改變未知數的係數的比.

首先,分出假分數 $\frac{127}{52}$ 的整數部分:

$$\frac{127}{52}=2+\frac{23}{52}.$$

用等於 $\frac{23}{52}$ 的分數 $\frac{1}{\frac{52}{23}}$ 來代替眞分數 $\frac{23}{52}$. 我們得到:

$$\frac{127}{52}=2+\frac{1}{\frac{52}{23}}.$$

把所得分母的假分數 $\frac{52}{23}$,也作同樣的改變:

$$\frac{52}{23}=2+\frac{6}{23}=2+\frac{1}{\frac{23}{6}}.$$

現在，原來的分數已可化成這樣的形式

$$\frac{127}{52}=2+\cfrac{1}{2+\cfrac{1}{\frac{23}{6}}}.$$

對於分數 $\frac{23}{6}$ 再作同樣的演算：

$$\frac{23}{6}=3+\frac{5}{6}=3+\frac{1}{\frac{6}{5}}.$$

於是

$$\frac{127}{52}=2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{\frac{6}{5}}}}.$$

分出假分數 $\frac{6}{5}$ 的整數部分：

$$\frac{6}{5}=1+\frac{1}{5},$$

我們得到最後的結果：

$$\frac{127}{52}=2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1+\frac{1}{5}}}}.$$

我們得到了叫做有限連分數或有限連鎖分數的式子．去掉這個連分數的最後一個分數五分之一，將所得的新連分數化成普通分數，並且從原來的分數 $\frac{127}{52}$ 減去它：

$$2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1}}}=2+\cfrac{1}{2+\cfrac{1}{4}}=2+\frac{4}{9}=\frac{22}{9},$$

$$\frac{127}{52}-\frac{22}{9}=\frac{1143-1144}{52\cdot 9}=-\frac{1}{52\cdot 9}.$$

把所得的式子通分，並且去掉分母；則

$$127\cdot 9-52\cdot 22+1=0.$$

把所得的等式和方程式

$$127x-52y+1=0$$

相比較，得 $x=9$，$y=22$ 是這個方程式的一組解，並且依照定理它的一切解必包括在級數

$$x=9+52t,\quad y=22+127t\quad (t=0,\pm 1,\pm 2,\cdots\cdots)$$

裏面。

所得的結果提供出這樣的觀念，即在一般的情況，要求方程式

$$ax+by+c=0$$

的整數解，就應當將未知數係數的比化成連分數，去掉它的最後一個分數，並且完成上面所作的類似的計算。

爲了證明這個命題，必須用到連分數的某些性質。

我們來研究既約分數 $\frac{a}{b}$，用 q_1 表示 a 除以 b 的商，用 r_2 表示餘數。則得

$$a=q_1b+r_2,\quad r_2<b.$$

其次，設 q_2 是 b 除以 r_2 的商，r_3 是餘數。則

$$b=q_2r_2+r_3,\quad r_3<r_2,$$

同樣

$$r_2=q_3r_3+r_4,\quad r_4<r_3,$$
$$r_3=q_4r_4+r_5,\quad r_5<r_4,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

數值 $q_1, q_2, \cdots\cdots$ 叫做**部分商**. 上面引用的構成部分商的過程叫做**歐幾里得算法**. 除得的餘數 $r_2, r_3, \cdots\cdots$ 適合於不等式

$$b>r_2>r_3>r_4>\cdots\cdots\geqslant 0, \tag{5}$$

就是，它們構成一個非負數的遞降數列.

因爲這些非負數的整數不超過 b，個數不能無限，所以在過程中的某一步，部分商的構成就終止了，由此以後輪到的餘數 r 就變成了零. 設 r_n 是數列(5)中最後一個不等於零的餘數，則 $r_{n+1}=0$，而歐幾里得算法對於數整 a 和 b 具有這樣的形式

$$\left.\begin{aligned} a&=q_1b+r_2,\\ b&=q_2r_2+r_3,\\ r_2&=q_3r_3+r_4,\\ &\cdots\cdots\cdots\cdots\\ r_{n-2}&=q_{n-1}r_{n-1}+r_n,\\ r_{n-1}&=q_nr_n. \end{aligned}\right\} \tag{6}$$

我們將所得的等式改寫成這樣形式：

$$\frac{a}{b}=q_1+\frac{1}{\frac{b}{r_2}},$$

$$\frac{b}{r_2}=q_2+\frac{1}{\frac{r_2}{r_3}},$$

…………………

$$\frac{r_{n-2}}{r_{n-1}}=q_{n-1}+\cfrac{1}{\cfrac{r_{n-1}}{r_n}},$$

$$\frac{r_{n-1}}{r_n}=q_n.$$

用這些等式中第二行的相當值來代替第一行的$\frac{b}{r_2}$，用第三行的相當值來代替第二行的$\frac{r_2}{r_3}$，這樣做下去，我們得到$\frac{a}{b}$化成的連分數，

$$\frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{\ddots}{+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}}}.$$

在連分數中，從某一部分開始，把在它以後的全部去掉，這樣得到的式子，叫做連分數的**近似分數**．第一近似分數 δ_1 是由去掉從 $\frac{1}{q_2}$ 起的一切部分得到的：

$$\delta_1=q_1<\frac{a}{b}.$$

第二近似分數 δ_2，是由去掉從 $\frac{1}{q_3}$ 起的一切部分得到的：

$$\delta_2=q_1+\frac{1}{q_2}>\frac{a}{b}.$$

同樣地

$$\delta_3=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}}<\frac{a}{b},$$

$$\delta_4=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4}}}>\frac{a}{b},$$

等等.

依據構成近似分數的方法,就產生明顯的不等式

$$\delta_1<\delta_3<\cdots\cdots<\delta_{2k-1}<\frac{a}{b};\ \delta_2>\delta_4>\cdots\cdots>\delta_{2k}>\frac{a}{b}.$$

我們將第 k 個近似分數 δ_k 寫成這樣的形式

$$\delta_k=\frac{P_k}{Q_k}\quad(1\leqslant k\leqslant n),$$

而求構成這個近似分數的分子和分母的法則. 我們改變起首幾個近似分數 δ_1, δ_2, δ_3 的形式:

$$\delta_1=q_1=\frac{q_1}{1}=\frac{P_1}{Q_1};\qquad P_1=q_1,\qquad Q_1=1;$$

$$\delta_2=q_1+\frac{1}{q_2}=\frac{q_1q_2+1}{q_2}=\frac{P_2}{Q_2};\qquad P_2=q_1q_2+1,\ Q_2=q_2;$$

$$\delta_3=q_1+\frac{1}{q_2+\frac{1}{q_3}}=q_1+\frac{q_3}{q_2q_3+1}=\frac{q_1q_2q_3+q_1+q_3}{q_2q_3+1}=\frac{P_3}{Q_3};$$

$$P_3=q_1q_2q_3+q_1+q_3,\quad Q_3=q_2q_3+1.$$

由此可得:

$$P_3=P_2q_3+P_1;\quad Q_3=Q_2q_3+Q_1.$$

我們用歸納法⊖來證明,相應於這個情況

$$P_k=P_{k-1}q_k+P_{k-2},\qquad Q_k=Q_{k-1}q_k+Q_{k-2},\qquad (7)$$

對於一切 $k\geqslant3$ 的數都成立.

事實上,設對於某一個 $k\geqslant3$ 的數等式 (7) 成立,從近似分數的定義直接就可以得出下面的情況: 在式子 δ_k 裏,用 $q_k+\frac{1}{q_{k+1}}$ 來代替 q_k, δ_k 就變成了 δ_{k+1}. 根據歸納法的假設,

⊖ 參看這一套叢書裏索明斯基(И. С. Соминский)著的'數學歸納法',國立技術理論書籍出版社,1950 年出版(已有中譯本, 高徹譯,中國青年出版社出版.——譯者註).

$$\delta_k=\frac{P_k}{Q_k}=\frac{P_{k-1}q_k+P_{k-2}}{Q_{k-1}q_k+Q_{k-2}}.$$

在這裏，用 $q_k+\frac{1}{q_{k+1}}$ 代替 q_k，我們得：

$$\delta_{k+1}=\frac{P_{k-1}\left(q_k+\frac{1}{q_{k+1}}\right)+P_{k-2}}{Q_{k-1}\left(q_k+\frac{1}{q_{k+1}}\right)+Q_{k-2}}=\frac{P_k+\frac{1}{q_{k+1}}P_{k-1}}{Q_k+\frac{1}{q_{k+1}}Q_{k-1}}$$

$$=\frac{P_kq_{k+1}+P_{k-1}}{Q_kq_{k+1}+Q_{k-1}}.$$

由此，因爲 $\delta_{k+1}=\frac{P_{k+1}}{Q_{k+1}}$，得

$$P_{k+1}=P_kq_{k+1}+P_{k-1},\quad Q_{k+1}=Q_kq_{k+1}+Q_{k-1}.$$

這樣一來，從等式(7)對於某一個 $k\geqslant 3$ 的數成立，得到對於 $k+1$ 它也成立。而且對於 $k=3$ 等式(7)已成立，於是它對於一切 $k\geqslant 3$ 的數都成立的正確性就確定了。

現在我們來證明，相鄰接的兩個近似分數的差 $\delta_k-\delta_{k-1}$ 適合於關係

$$\delta_k-\delta_{k-1}=\frac{(-1)^k}{Q_kQ_{k-1}}\qquad(k>1).\qquad(8)$$

事實上，

$$\delta_k-\delta_{k-1}=\frac{P_k}{Q_k}-\frac{P_{k-1}}{Q_{k-1}}=\frac{P_kQ_{k-1}-Q_kP_{k-1}}{Q_kQ_{k-1}}.$$

用公式(7)改變所得分數的分子，

$$P_kQ_{k-1}-Q_kP_{k-1}$$
$$=(P_{k-1}q_k+P_{k-2})Q_{k-1}-(Q_{k-1}q_k+Q_{k-2})P_{k-1}$$
$$=-(P_{k-1}Q_{k-2}-Q_{k-1}P_{k-2}).$$

在這括弧裏的式子，可從原來的式子用 $k-1$ 代替 k 得出來。

對於所得到的式子，重複這樣的改變，顯然地，我們得到一連串等式：

$$\begin{aligned}P_kQ_{k-1}-Q_kP_{k-1}&=(-1)(P_{k-1}Q_{k-2}-Q_{k-1}P_{k-2})\\&=(-1)^2(P_{k-2}Q_{k-3}-Q_{k-2}P_{k-3})\\&=\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\&=(-1)^{k-2}(P_2Q_1-Q_2P_1)\\&=(-1)^{k-2}(q_1q_2+1-q_2q_1)\\&=(-1)^{k-2}.\end{aligned}$$

由此可知，

$$\delta_k-\delta_{k-1}=\frac{P_kQ_{k-1}-Q_kP_{k-1}}{Q_kQ_{k-1}}=\frac{(-1)^{k-2}}{Q_kQ_{k-1}}=\frac{(-1)^k}{Q_kQ_{k-1}}.$$

若 $\frac{a}{b}$ 化成的連分數具有 n 個部分，則第 n 個近似分數 δ_n 就和 $\frac{a}{b}$ 一致．應用公式(8)，在 $k=n$ 的時候，我們得：

$$\delta_n-\delta_{n-1}=\frac{(-1)^n}{Q_nQ_{n-1}},$$

$$\frac{a}{b}-\delta_{n-1}=\frac{(-1)^n}{bQ_{n-1}}. \qquad (9)$$

現在我們回到解方程式

$$ax+by+c=0,\ (a,b)=1. \qquad (10)$$

我們把關係(9)改寫成這樣形式

$$\frac{a}{b}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^n}{bQ_{n-1}}.$$

通分母並且把它消去，我們得：

$$aQ_{n-1}-bP_{n-1}=(-1)^n,$$

$$aQ_{n-1}+b(-P_{n-1})+(-1)^{n-1}=0.$$

用 $(-1)^{n-1}c$ 乘這個關係式，則

$$a[(-1)^{n-1}cQ_{n-1}]+b[(-1)^{n}cp_{n-1}]+c=0.$$

由此可見，這一對數 $[x_0\ y_0]$，

$$x_0=(-1)^{n-1}cQ_{n-1},\quad y_0=(-1)^{n}cP_{n-1}, \qquad (11)$$

是方程式(10)的一組解，並且根據定理，這個方程式的一切解具有這樣的形式：

$$x=(-1)^{n-1}cQ_{n-1}-bt,\quad y=(-1)^{n}cP_{n-1}+at$$
$$(t=0,\pm1,\pm2,\cdots\cdots).$$

上面所得的結果，完全解決了關於求二元一次方程式的一切整數解的問題。現在我們來進行研究某些二次方程式。

三　三元二次方程式的範例

〔範例 1〕 我們來考察三元二次方程式：

$$x^2+y^2=z^2. \qquad (12)$$

這個方程式的整數的幾何的解，可以這樣說明，求一切畢達果拉斯三角形㊀，就是直角三角形，在那裏，兩條直角邊 x，y 既是整數，斜邊也是整數。

用 d 表示 x 和 y 的最大公因數：$d=(x,y)$。則

$$x=x_1d,\quad y=y_1d,$$

而方程式(12)取這樣形式

$$x_1^2d^2+y_1^2d^2=z^2.$$

由此可知，z^2 可以被 d^2 除盡，也就是，z 是 d 的倍數：$z=z_1d$.

現在方程式(12)可以寫成這樣形式

㊀ 即勾股形；據我國古算書'周髀算經'，是商高發現的。——譯者註

$$x_1^2 d^2 + y_1^2 d^2 = z_1^2 d^2;$$

除以 d^2，我們得：

$$x_1^2 + y_1^2 = z_1^2.$$

我們得到了和原方程式一樣的形式，並且，現在 x_1 和 y_1 兩個數不具有 1 以外的公因數．這樣一來，方程式（12）的解可以限於 x 和 y 是互質數的這種情況． 因而，設 $(x,y)=1$，於是 x 和 y 兩個數中至少有一個（例如 x）必定是奇數．移 y^2 到方程式(12)的右邊，我們得：

$$x^2 = z^2 - y^2; \quad x^2 = (z+y)(z-y). \qquad (13)$$

用 d_1 表示兩個式子 $z+y$ 和 $z-y$ 的最大公因數．則

$$z+y = ad_1, \quad z-y = bd_1, \qquad (14)$$

這兒 a 和 b 是互質數．

將 $z+y$ 和 $z-y$ 的値代入(13)，我們得：

$$x^2 = abd_1^2.$$

因爲 a 和 b 兩數沒有公因數，則所得的這個等式只有在 a 和 b 都是平方數的情況才可能㊀：

$$a = u^2, \quad b = v^2.$$

那時候
$$x^2 = u^2v^2d_1^2,$$
而
$$x = uvd_1. \qquad (15)$$

現在，我們由等式(14)求 y 和 z．把這兩個等式相加，得：

$$2z = ad_1 + bd_1 = u^2d_1 + v^2d_1; \quad z = \frac{u^2+v^2}{2} d_1. \qquad (16)$$

從等式(14)中的第一個減去第二個，得：

㊀ 大家知道，兩個互質數的積，只有在每一個因數都是完全平方數的時候它才能是一個完全平方數

$$2y=ad_1-bd_1=u^2d_1-v^2d_1;\quad y=\frac{u^2-v^2}{2}d_1. \qquad (17)$$

由於 x 是奇數，由(15)我們得 u, v 和 d_1 也都是奇數．不但這樣，還得 $d_1=1$，因爲若不這樣，則從等式

$$x=uvd_1 \text{ 和 } y=\frac{u^2-v^2}{2}d_1$$

將要得出 x 和 y 兩個數具有公因數 $d_1\neq1$，這和它們是互質數的假設相矛盾．u 和 v 兩個數和互質數 a 和 b 的關係，有等式

$$a=u^2,\quad b=v^2,$$

因而它們本身也是互質數；並且 $v<u$，因爲 $b<a$，這由等式(14)可以看得很明白．

以 $d_1=1$ 代入等式(15)、(17)和(16)中，我們就得公式：

$$x=uv,\quad y=\frac{u^2-v^2}{2},\quad z=\frac{u^2+v^2}{2}, \qquad (18)$$

給出用互質的奇數 u 和 v ($v<u$) 表示的、沒有公因數的三個正整數 x, y, z，它們是適合方程式(12)的．直接將 x, y 和 z 代入方程式 (12) 中，很容易證明，取任何的 u 和 v (18) 都適合於這個方程式．

對於開始的幾個 u 和 v 的值，公式 (18) 卽變成下面常見的等式：

$$3^2+4^2=5^2 \qquad (v=1, u=3),$$
$$5^2+12^2=13^2 \qquad (v=1, u=5),$$
$$15^2+8^2=17^2 \qquad (v=3, u=5).$$

恰如剛才所討論的，公式(18)只給出方程式

$$x^2+y^2=z^2$$

在 x, y 和 z 三數沒有公因數時的那些組解．這個方程式的其

餘各組正整數解，可由包含在公式（18）中的解乘以公因數 d 得出來。

應用我們得到方程式（12）的一切解的同樣方法，也可以得到同一類型的別的方程式的一切解。

〔範例2〕　求方程式

$$x^2+2y^2=z^2 \tag{19}$$

的一切正整數解，其中 x, y, z 是兩兩互質的。

我們注意，若 x, y, z 是方程式（19）的一組解，並且 x, y, z 不具有1以外的公因數，則它們就必是兩兩互質的。事實上，若 x 和 y 是質數 $p>2$ 的倍數，則從等式

$$\left(\frac{x}{p}\right)^2+2\left(\frac{y}{p}\right)^2=\left(\frac{z}{p}\right)^2$$

可以得出 z 也是 p 的倍數，因為等式的左邊是一個整數。在 x 和 z 或 y 和 z 都能夠被 p 除得盡，情形也是一樣。

我們還得注意，要使 x, y, z 的最大公因數等於1，x 必須是一個奇數。事實上，若 x 是一個偶數，則方程式（19）的左邊就是偶數，就是說 z 也是偶數。但這時 x^2 和 z^2 將被4除盡。因而 $2y^2$ 也應當被4除得盡，換句話說，y 也應當是一個偶數。這就是說，若 x 是一個偶數，則 x, y, z 全都得是偶數。因此，在一組解中沒有1以外的公因數，則 x 必須是一個奇數。由此還可以得到，z 也必須是一個奇數。將 x^2 移到右邊，我們得：

$$2y^2=z^2-x^2=(z+x)(z-x).$$

但是，$z+x$ 和 $z-x$ 具有公因數2。實際上，設它們的公因數為 d，則

$$z+x=kd,\quad z-x=ld,$$

這兒 k 和 l 是兩個整數．加和減這兩個等式，我們得：

$$2z=d(k+l),\quad 2x=d(k-l).$$

但 z 和 x 是奇數並且是互質數，因而 $2x$ 和 $2z$ 的最大公因數必得是 2．由此可見，$d=2$．

由此，或 $\frac{z+x}{2}$ 或 $\frac{z-x}{2}$ 是奇數，因而或兩個數

$$z+x \text{ 和 } \frac{z-x}{2}$$

是互質數，或兩個數

$$\frac{z+x}{2} \text{ 和 } z-x$$

是互質數．在第一種情形，由等式

$$(z+x)\frac{z-x}{2}=y^2,$$

得到

$$z+x=n^2,\quad z-x=2m^2;$$

而在第二種情形，由等式

$$\frac{z+x}{2}(z-x)=y^2,$$

得到

$$z+x=2m^2,\quad z-x=n^2;$$

這兒 n 和 m 都是整數，m 是奇數，並且 $n>0, m>0$．對於 x 和 z 解這兩組方程式系，並且求 y，我們得到，或是

$$z=\frac{1}{2}(n^2+2m^2),\quad x=\frac{1}{2}(n^2-2m^2),\quad y=mn;$$

或是

$$z=\frac{1}{2}(n^2+2m^2),\quad x=\frac{1}{2}(2m^2-n^2),\quad y=mn;$$

這兒 m 是奇數．聯合這兩組表示 x,y,z 的解的公式，我們得

一般的公式

$$x=\pm\frac{1}{2}(n^2-2m^2),\quad y=mn,\quad z=\frac{1}{2}(n^2+2m^2),$$

這兒 m 是奇數. 但,要使得 z 和 x 都是整數,必須使 n 是偶數. 設 $n=2b$ 和 $m=a$,我們最後得到了**給與方程式 (19) 一切沒有大於 1 的公因數的正整數解 x,y,z 的一般公式**

$$x=\pm(a^2-2b^2),\quad y=2ab,\quad z=a^2+2b^2,\qquad (19')$$

這兒 a 和 b 是互質的正整數,並且 a 是奇數. 在這些條件之下,a 和 b 的值可以任意選定,但要使得 x 是正的. 公式(19′)實際上給出了一切兩兩互質的正整數解 x,y,z,因爲,一方面我們證明了,在這種情形之下,x,y,z 必然由公式(19′)來表示,而在另一方面,若我們給了適合我們條件的兩個數 a 和 b,則 x,y,z 必確是互質的,並且是方程式(19)的解.

四 $x^2-Ay^2=1$ 型的方程式. 求這種方程式的一切解

現在,我們來研究具有形式

$$x^2-Ay^2=1\qquad (20)$$

的二元二次方程式的整數解,這兒 A 是正整數而不是完全平方數. 爲了求出解這種方程式的門徑,我們先來介紹將形式是$\sqrt{A}$ 的無理數化成連分數的方法. 由歐幾里得算法,我們可以把一切有理數化成有限連分數. 對於無理數却是另外一回事. 相應於無理數的是無限連分數. 例如,我們來將無理數$\sqrt{2}$ 化成連分數.

改變顯而易見的恆等式

$$(\sqrt{2}-1)(\sqrt{2}+1)=1$$

爲

$$\sqrt{2}-1=\frac{1}{\sqrt{2}+1},$$

$$\sqrt{2}-1=\frac{1}{2+(\sqrt{2}-1)};$$

分母中所得到的差$\sqrt{2}-1$，用相等的同樣的式子

$$\frac{1}{2+(\sqrt{2}-1)}$$

表示，我們就得：

$$\sqrt{2}-1=\cfrac{1}{2+\cfrac{1}{2+(\sqrt{2}-1)}};\quad \sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+(\sqrt{2}-1)}}.$$

再一次用同樣的分數來代替末了一個分母括弧中的數，則

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+(\sqrt{2}-1)}}}.$$

繼續這個步驟，我們得到下面$\sqrt{2}$化成的無限連分數：

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\ddots}}}}. \qquad (21)$$

我們須注意，上面所用的化連分數方法是利用恆等式

$$(\sqrt{m^2+1}-m)(\sqrt{m^2+1}+m)=1$$

作根據的，並不能對一切無理數 $\sqrt{A}$ 都適用。 這個方法

很明白地，可以應用在這種情形，就是當整數 A 能夠表示成 $A=m^2+1$，m 是零以外的任何整數的時候（在特殊情形，當 $m=1$ 的時候，得 $\sqrt{2}$ 的展開式，當 $m=2$，即得 $\sqrt{5}$ 的展開式等等）．但是，一般情形的化 $\sqrt{A}$ 成無限連分數的比較簡單的方法㊀，是大家已經知道了的．

和在以前的有限連分數的情形一樣，我們把無限連分數(21)也改變成近似分數列 $\delta_1, \delta_2, \delta_3, \cdots\cdots$

$$\begin{aligned} &\delta_1=1, && \delta_1<\sqrt{2}; \\ &\delta_2=1+\frac{1}{2}=\frac{3}{2}, && \delta_2>\sqrt{2}; \\ &\delta_3=1+\cfrac{1}{2+\cfrac{1}{2}}=\frac{7}{5}, && \delta_3<\sqrt{2}; \\ &\delta_4=\cdots\cdots=\frac{17}{12}, && \delta_4>\sqrt{2} \end{aligned} \tag{22}$$

等等．

從構成近似分數的方法即得，

$$\delta_1<\delta_3<\cdots\cdots<\sqrt{2},$$

$$\delta_2>\delta_4>\cdots\cdots>\sqrt{2}.$$

一般地，若已知某個無理數 α 的無限連分數展開式

$$\alpha=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots}},$$

㊀ 參看，例如，阿諾爾德 (И. В. Арнольда) 的'數論'第六章（蘇俄教育部國立教科書出版社，1939 年出版）；或辛勁 (А. Я. Хинчин) 的'連分數'（國立技術理論書籍出版社，1949年出版）．

則對於這些近似分數，不等式

$$\delta_1<\delta_3<\cdots<\delta_{2k+1}<\cdots<\alpha<\cdots<\delta_{2k}<\cdots<\delta_4<\delta_2 \quad (23)$$

成立．我們將近似分數 δ_k 表示成這樣形式：

$$\delta_k=\frac{P_k}{Q_k}.$$

以前對於有限連分數所得到的關係(7)

$$P_k=P_{k-1}q_k+P_{k-2}, \quad Q_k=Q_{k-1}q_k+Q_{k-2}$$

對於無限連分數也成立；因爲在推出這個關係的時候，我們並沒有利用到這連分數是有限的這個性質． 因此，在相鄰的兩個近似分數之間的關係(8)也一樣地成立：

$$\delta_k-\delta_{k-1}=\frac{(-1)^k}{Q_kQ_{k-1}}. \quad (24)$$

例如，對於$\sqrt{2}$化成的連分數的近似分數，當 $k=3$ 和 $k=4$ 的時候，從(22)我們就得：

$$\delta_3-\delta_2=\frac{7}{5}-\frac{3}{2}=\frac{-1}{10},$$

$$\delta_4-\delta_3=\frac{17}{12}-\frac{7}{5}=\frac{1}{60},$$

這，當然和(24)所指出的結果一致．

從 (24)，特別可得到，

$$\delta_{2k}-\delta_{2k+1}=-(\delta_{2k+1}-\delta_{2k})=-\frac{(-1)^{2k+1}}{Q_{2k+1}Q_{2k}}=\frac{1}{Q_{2k+1}Q_{2k}}.$$

現在，我們來證明不等式

$$0<P_{2k}-\alpha Q_{2k}<\frac{1}{Q_{2k+1}} \quad (25)$$

是正確的．實際上，這個不等式的左邊立刻可以得出來，因爲依照(23)

$$\alpha<\delta_{2k}=\frac{P_{2k}}{Q_{2k}};\quad \alpha Q_{2k}<P_{2k};\quad 0<P_{2k}-\alpha Q_{2k}.$$

證明不等式(25)的右邊也不困難，由(23)

$$\delta_{2k+1}<\alpha<\delta_{2k};$$

因而

$$\delta_{2k}-\alpha<\delta_{2k}-\delta_{2k+1}=\frac{1}{Q_{2k}Q_{2k+1}}.$$

由此，用 $\frac{P_{2k}}{Q_{2k}}$ 代替 δ_{2k}，我們得：

$$\frac{P_{2k}}{Q_{2k}}-\alpha<\frac{1}{Q_{2k}Q_{2k+1}}.$$

用 Q_{2k} 乘這個不等式，我們就得到所要求的結果

$$P_{2k}-\alpha Q_{2k}<\frac{1}{Q_{2k+1}}.$$

現在，把已經得到的結果應用到解方程式

$$x^2-2y^2=1. \qquad (26)$$

我們改變這個方程式的左邊：

$$x^2-2y^2=(x-\sqrt{2}y)(x+\sqrt{2}y).$$

設 $x=P_{2k}$ 和 $y=Q_{2k}$，這兒 P_{2k} 和 Q_{2k} 是$\sqrt{2}$ 化成的連分數的相應的近似分數的分子和分母．因而

$$P_{2k}^2-2Q_{2k}^2=(P_{2k}-\sqrt{2}Q_{2k})(P_{2k}+\sqrt{2}Q_{2k}). \qquad (27)$$

得出的等式的左邊也就是右邊是個整數． 我們來證明，這個整數大於零而小於2，因而就等於1．對於這一點，我們應用不等式(25)，取 $\alpha=\sqrt{2}$：

$$0<P_{2k}-\sqrt{2}\,Q_{2k}<\frac{1}{Q_{2k+1}}. \qquad (28)$$

由此可見，(27)右邊的兩個因數都是正的，就是

$$P_{2k}^2-2Q_{2k}^2>0.$$

在另一邊，

$$P_{2k}-\sqrt{2}Q_{2k}<\frac{1}{Q_{2k+1}}=\frac{1}{Q_{2k}q_{2k+1}+Q_{2k-1}}$$

$$=\frac{1}{2Q_{2k}+Q_{2k-1}}<\frac{1}{2Q_{2k}}.$$

但由(23)

$$\delta_{2k}=\frac{P_{2k}}{Q_{2k}}>\sqrt{2}.$$

因而

$$\sqrt{2}Q_{2k}<P_{2k},$$

$$P_{2k}+\sqrt{2}Q_{2k}<2P_{2k},$$

並且，對於等式(27)右邊的兩個因數，我們得到兩個不等式：

$$P_{2k}-\sqrt{2}Q_{2k}<\frac{1}{2Q_{2k}},$$

$$P_{2k}+\sqrt{2}Q_{2k}<2P_{2k}.$$

將這兩個不等式相乘，得：

$$P_{2k}^2-2Q_{2k}^2<\frac{P_{2k}}{Q_{2k}}.$$

應用不等式(28)，因而我們得：

$$P_{2k}^2-2Q_{2k}^2<\frac{\sqrt{2}Q_{2k}+\frac{1}{Q_{2k+1}}}{Q_{2k}}=\sqrt{2}+\frac{1}{Q_{2k}Q_{2k+1}};$$

而因為對於所有的 $k\geqslant 1$

$$\frac{1}{Q_{2k}Q_{2k+1}}\leqslant\frac{1}{Q_2Q_3}=\frac{1}{10},$$

於是，

$$P_{2k}^2-2Q_{2k}^2<\sqrt{2}+\frac{1}{10}<2.$$

這樣一來，我們就證明了，整數 $P_{2k}^2-2Q_{2k}^2$ 對於任何 $k\geqslant1$，都適合於不等式

$$0<P_{2k}^2-2Q_{2k}^2<2.$$

因而，

$$P_{2k}^2-2Q_{2k}^2=1,$$

就是 $x=P_{2k}, y=Q_{2k}$ 兩個數，在任何 $k\geqslant1$ 的時候，都給與方程式

$$x^2-2y^2=1$$

的解。

我們到這時候還不曾知道，我們所已求得的方程式(26)的解是不是這個方程式的一切解。

現在自然就會提出這樣的問題，當 $A>0$ 是整數而 $\sqrt{A}$ 是無理數的時候，怎樣得到方程式

$$x^2-Ay^2=1 \qquad (29)$$

的一切整數解 x 和 y。我們來指明，假如方程式 (29) 至少有一組解是已知的時候，這是可能做到的。在方程式 (26) 的例中，我們已經見到這樣的方程式是有解的。我們暫時不問，方程式(29)是不是至少具有一組與整數解 $x=1, y=0$ 不同的整數解，我們現在要問：怎樣從方程式 (29) 的一組一定的解，這我們把它叫做最小解的，求出它的一切解來。

我們假定方程式 (29) 具有一組非常解 $[x_0, y_0]$，$x_0>0$，$y_0>0$，

$$x_0^2-Ay_0^2=1. \qquad (30)$$

(我們記好，把適合於方程式的一對整數 $[x_0, y_0]$ 叫做一組解)．若 $\sqrt{A}>0$，在 $x=x_0$，$y=y_0$ 時，二項式 $x+\sqrt{A}y$ 的值，是將方程式 (29) 的一切可能有的 (異於零的) 正整數解代其中的 x 和 y 所得值中的最小的一個，則我們叫這組解 $[x_0, y_0]$ 是**最小解**．例如對於方程式 (26)，最小解就是 $x=3, y=2$；因爲在 x 和 y 取這種值的時候，$x+\sqrt{2}y$ 就取數值 $3+2\sqrt{2}$，而方程式(26)並不存在别的最小解．這只消試去選取小的正整數，使得它又是解，並且又使 $x+\sqrt{2}y$ 的值不大於 $3+2\sqrt{2}$，就可以立刻看出來．實際上，就大小說，方程式的次一組解的值是 $x=17$，$y=12$，很明白地，$17+12\sqrt{2}$ 大於 $3+2\sqrt{2}$．我們還得注意，**並不存在方程式(29)的兩組最小解**．反過來，我們假定，有兩組解 $[x_1, y_1]$ 和 $[x_2, y_2]$，它們都給二項式 $x+\sqrt{A}y$ 同樣的值．則

$$x_1+\sqrt{A}y_1=x_2+\sqrt{A}y_2, \tag{31}$$

但 $\sqrt{A}$ 是無理數，而 x_1, y_1, x_2, y_2 是整數．那末，從等式 (31)，直接可得到

$$x_1-x_2=(y_2-y_1)\sqrt{A},$$

這是不可能的，因爲 x_1-x_2 是整數，$(y_2-y_1)\sqrt{A}$ 是整數和無理數的積必是無理數，而整數不可能又是無理數． 若 $x_1=x_2$ 和 $y_1=y_2$，這個矛盾就消失了；換句話說，我們所取的不是兩個不同的解而是一個．由此可知，若最小解存在，那就只有一組．我們現在還得注意到方程式(29)的解的一個很重要的性質．設 $[x_1, y_1]$ 是方程式 (29) 的解，則

$$x_1^2-Ay_1^2=1$$

或

$$(x_1+\sqrt{A}y_1)(x_1-\sqrt{A}y_1)=1. \qquad (32)$$

現在，將等式(32)的兩邊自乘 n 次 (n 是正整數)：

$$(x_1+\sqrt{A}y_1)^n(x_1-\sqrt{A}y_1)^n=1. \qquad (33)$$

依照二項式乘方的法則，實行乘方，我們得：

$$(x_1+\sqrt{A}y_1)^n=x_1^n+nx_1^{n-1}\sqrt{A}y_1$$

$$+\frac{n(n-1)}{2}x_1^{n-2}Ay_1^2+\cdots\cdots+(\sqrt{A})^ny_1^n=x_n+\sqrt{A}y_n, \qquad (34)$$

這兒 x_n 和 y_n 都是整數，因為依照二項式法則，展開式的第一項、第三項，一般說來，一切的奇數項都是整數，而偶數項都是整數乘以$\sqrt{A}$. 分別集合整數項和$\sqrt{A}$的整倍數的項，我們就得等式(34). 兩個數 x_n 和 y_n 照我們就要證明的，也是方程式(29)的解. 實際上，從等式(34)，改變$\sqrt{A}$的符號，我們就得等式

$$(x_1-\sqrt{A}y_1)^n=x_n-\sqrt{A}y_n. \qquad (35)$$

將等式(34)和(35)相乘並且應用等式(33)，我們最後得到

$$(x_1+\sqrt{A}y_1)^n(x_1-\sqrt{A}y_1)^n=(x_n+\sqrt{A}y_n)(x_n-\sqrt{A}y_n)$$

$$=x_n^2-Ay_n^2=1, \qquad (36)$$

換句話說，$[x_n, y_n]$ 也是方程式(29)的解.

現在我們能夠證明關於方程式(29)的解的基本定理.

〔定理 2〕 方程式(29)

$$x^2-Ay^2=1$$

的一切解，在 A 是正數而$\sqrt{A}$是無理數的時候，具有形式 $[\pm x_n, \pm y_n]$，這兒

$$\left.\begin{aligned} x_n&=\frac{1}{2}[(x_0+y_0\sqrt{A})^n+(x_0-y_0\sqrt{A})^n],\\ y_n&=\frac{1}{2\sqrt{A}}[(x_0+y_0\sqrt{A})^n-(x_0-y_0\sqrt{A})^n],\end{aligned}\right\}\qquad(37)$$

而 $[x_0\ y_0]$ 是最小解.

〔證明〕 假若不是這樣，我們假定方程式 (29) 存在着正整數解 $[x', y']$，它使得等式

$$x'+\sqrt{A}y'=(x_0+\sqrt{A}y_0)^n \qquad (38)$$

對於任何的正整數 n 都不成立．我們來觀察數列

$$x_0+\sqrt{A}\,y_0,(x_0+\sqrt{A}\,y_0)^2,(x_0+\sqrt{A}\,y_0)^3,\cdots\cdots$$

因爲 $x_0\geqslant1, y_0\geqslant1$ 和 $x_0+\sqrt{A}\,y_0>1$，所以這是一個無限遞增的正數列．由於 $[x_0\ y_0]$ 是最小解，依照最小解的定義

$$x'+\sqrt{A}y'>x_0+\sqrt{A}y_0.$$

因此，必可求得整數 $n\geqslant1$，使

$$(x_0+\sqrt{A}y_0)^n<x'+\sqrt{A}y'<(x_0+\sqrt{A}y_0)^{n+1}. \quad (39)$$

但是由於

$$(x_0+\sqrt{A}y_0)(x_0-\sqrt{A}\,y_0)=x_0^2-Ay_0^2=1>0,$$

所以 $$x_0-\sqrt{A}y_0>0.$$

因爲將不等式 (39) 的各項乘以同一個正數 $(x_0-\sqrt{A}y_0)^n$，所有不等式的方向不變，我們就有：

$$(x_0+\sqrt{A}y_0)^n(x_0-\sqrt{A}y_0)^n<(x'+\sqrt{A}y')(x_0-\sqrt{A}y_0)^n$$
$$<(x_0+\sqrt{A}y_0)^{n+1}(x_0-\sqrt{A}y_0)^n. \qquad (40)$$

因爲

$$(x_0+\sqrt{A}y_0)^n(x_0-\sqrt{A}y_0)^n=(x_0^2-Ay_0^2)^n=1, \quad (41)$$

所以

$$(x_0+\sqrt{A}y_0)^{n+1}(x_0-\sqrt{A}y_0)^n=x_0+\sqrt{A}y_0\text{.} \quad (42)$$

此外，

$$(x'+\sqrt{A}y')(x_0-\sqrt{A}y_0)^n=(x'+\sqrt{A}y')(x_n-\sqrt{A}y_n)$$
$$=x'x_n-Ay'y_n+\sqrt{A}(y'x_n-x'y_n)$$
$$=\bar{x}+\sqrt{A}\,\bar{y}, \quad (43)$$

這兒 $\bar{x}$ 和 $\bar{y}$ 是整數，並且

$$x_n-\sqrt{A}y_n=(x_0-\sqrt{A}y_0)^n.$$

應用關係(41)，(42)，(43) 以及不等式(40)，我們得到不等式

$$1<\bar{x}+\sqrt{A}\,\bar{y}<x_0+\sqrt{A}y_0. \quad (44)$$

我們來證明這一對整數 $\bar{x}$ 和 $\bar{y}$ 必定是方程式(29)的解．實際上，將等式(43)即等式

$$\bar{x}+\sqrt{A}\bar{y}=(x'+\sqrt{A}y')(x_0-\sqrt{A}y_0)^n \quad (45)$$

和從(43)改變 $\sqrt{A}$ 的符號，直接得出來的等式

$$\bar{x}-\sqrt{A}\bar{y}=(x'-\sqrt{A}y')(x_0+\sqrt{A}y_0)^n, \quad (46)$$

各邊相乘，我們就得：

$$(\bar{x}+\sqrt{A}\,\bar{y})(\bar{x}-\sqrt{A}\,\bar{y})=\bar{x}^2-A\bar{y}^2$$
$$=(x'+\sqrt{A}y')(x'-\sqrt{A}y')(x_0+\sqrt{A}y_0)^n(x_0-\sqrt{A}y_0)^n$$
$$=(x'^2-Ay'^2)(x_0^2-Ay_0^2)^n=1, \quad (47)$$

因爲 $[x',y']$ 和 $[x_0\ y_0]$ 都是方程式(29)的解．末了，我們來證明，$\bar{x}>0$ 和 $\bar{y}>0$．首先很明白地，$\bar{x}$ 不等於零．實際上，若 $\bar{x}=0$，則從等式(47)我們就有：

$$-A\bar{y}^2=1,$$

但因爲 $A>0$，這是不可能的．其次，若 $\bar{y}=0$，則 $\bar{x}^2=1$，但從不等式(44) $\bar{x}>1$，所以這也是不可能的．最後我們注意，$\bar{x}$

和$\bar{y}$的符號必須是相同的．實際上，若假定 $\bar{x}$ 和 $\bar{y}$ 的符號不相同，則$\bar{x}$ 和 $-\bar{y}$ 就必具有相同的符號． 這時若我們比較 $\bar{x}+\sqrt{A}\bar{y}$和$\bar{x}-\sqrt{A}\,\bar{y}$兩個數的絕對值，則這兩個數當中，第一個數的絕對值必小於第二個數的絕對值，因爲在第一個數中是從兩個同符號的數中的一個減去他一個，而在另一個却是相加．但我們還知道，

$$\bar{x}+\sqrt{A}\,\bar{y}>1;$$

卽，$\bar{x}-\sqrt{A}\bar{y}$的絕對值一樣地也大於 1．然而

$$(\bar{x}+\sqrt{A}\,\bar{y})(\bar{x}-\sqrt{A}\bar{y})=\bar{x}^2-A\bar{y}^2=1,$$

我們就得出了矛盾，因爲兩個數中每一個的絕對值都大於 1，這兩個數的積的絕對值應當也大於 1．由此可知，$\bar{x}$ 和 $\bar{y}$ 的符號相同並且$\bar{x}\neq 0$ 和 $\bar{y}\neq 0$．在這種情況，由不等式 (44) 已經立刻可以得到，

$$\bar{x}>0 \text{ 和 } \bar{y}>0.$$

由此可知，假定方程式

$$x^2-Ay^2=1,\quad A>0$$

存在着解 $[x',y']$，使得等式 (38) 對於任何的正整數 n 都不成立，我們就能造出這個方程式的一組解，$[\bar{x},\bar{y}]$，$\bar{x}>0$，$\bar{y}>0$，$\bar{x}$和$\bar{y}$是適合於不等式(44)的整數，這和最小解 $[x_0\ y_0]$ 的定義相矛盾．這樣，我們也已證明了，假定存在着不是由公式 (38) 所表示的解，就會引出矛盾來． 換句話說，我們證明了我們的方程式的一切解都能夠從公式(38)得出來．

由此，方程式(29)的任何解 $[x,y]$ 都可以從關係式

$$x+\sqrt{A}y=(x_0+\sqrt{A}y_0)^n,\quad n\geqslant 0 \qquad (48)$$

得到，這兒 $[x_0\ y_0]$ 是最小解．改變上面等式中 $\sqrt{A}$ 的符號，我們就得到等式

$$x-\sqrt{A}y=(x_0-\sqrt{A}y_0)^n. \qquad (49)$$

加減這兩個等式，並且相應地除以 2 或 $2\sqrt{A}$，我們得着：

$$\left.\begin{aligned} x=x_n&=\frac{1}{2}[(x_0+\sqrt{A}y_0)^n+(x_0-\sqrt{A}y_0)^n],\\ y=y_n&=\frac{1}{2\sqrt{A}}[(x_0+\sqrt{A}y_0)^n-(x_0-\sqrt{A}y_0)^n],\end{aligned}\right\} \qquad (50)$$

換句話說，我們得到了對於任何的解 $[x,y]$ 當 x 和 y 都是正數時的明確公式．若在 x_n 和 y_n 的前面取任意的符號，則從這個式子就得到所有的解．

例如，因爲我們在前面已經見到，方程式

$$x^2-2y^2=1$$

的最小解是 $x=3$, $y=2$，則這個方程式的一切解都包含在公式：

$$x_n=\frac{1}{2}[(3+2\sqrt{2})^n+(3-2\sqrt{2})^n],$$

$$y_n=\frac{1}{2\sqrt{2}}[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n]$$

裏面；從這兒，取 $n=1,2,3$，我們得到解：[3,2]，[17,12]，[99,70]．

我們注意，x_n 和 y_n 兩個數是以隨着 n 增長而以 $x_0+\sqrt{A}y_0$ 作公比的幾何級數的速度增長的；因爲由等式

$$(x_0+\sqrt{A}y_0)(x_0-\sqrt{A}y_0)=1$$

我們能夠推得

$$0<x_0-\sqrt{A}y_0<1,$$

也就是說，$(x_0-\sqrt{A}y_0)^n$ 隨着 n 的增長總是趨近於零.

現在我們注意，若方程式(29)至少具有一組非常解，——換句話說，至少有一組 $y\neq0$ 的解，則這個方程式就存在着一組最小解，而這時它的一切解都可以從公式(50)得出來. 當 A 是任意正整數而 $\sqrt{A}$ 是無理數的時候，關於這個方程式是否具有非常解的問題，我們曾經作暫時保留，沒有解決，現在却輪到它了.

五 二元二次方程式的一般情況

在這一節裏，我們來證明，對於 A 是任意的正整數而 $\sqrt{A}$ 是無理數時，方程式

$$x^2-Ay^2=1 \tag{51}$$

總具有非常解，——換句話說，存在着適合於這方程式的一對整數 x_0 和 y_0，x_0；$y_0\neq0$. 我們首先指明化任何正數成連分數的方法. 前面，爲了化成連分數我們曾經利用過 $\sqrt{2}$ 這個數的特殊性質. 設 α 是任意一個正數. 那末，總存在着一個整數，它小於或等於 α 而大於 $\alpha-1$. 這樣的數叫做 α 的整數部分，而用 $[\alpha]$ 來表示. α 和它的整數部分的差叫做 α 的分數部分而用 $\{\alpha\}$ 來表示. 從 α 的整數部分和分數部分的定義，立刻就得到它們中間的關係，就是：

$$\alpha-[\alpha]=\{\alpha\},$$

或

$$\alpha=[\alpha]+\{\alpha\}. \tag{52}$$

因爲一個數的分數部分是一個正數跟不超過它的最大整數之

間的差，所以分數部分總小於 1 而不是負的．例如，$\frac{27}{5}$ 的整數部分是 5，而它的分數部分是 $\frac{2}{5}$；$\sqrt{2}$ 的整數部分是 1，而分數部分等於 $\sqrt{2}-1$；$\sqrt[3]{52}$ 的整數部分是 3，而分數部分等於 $\sqrt[3]{52}-3$，等等．

由我們引用的正數 α 的整數部分和分數部分的定義，可以被利用來化這個數成連分數．設：

$$[\alpha]=q_1,\ \{\alpha\}=\frac{1}{\alpha_1},$$

則

$$\alpha=q_1+\frac{1}{\alpha_1}. \tag{53}$$

因爲 $\{\alpha\}$ 總小於 1，所以 α_1 總大於1．若 α 本身就是整數，則它的分數部分就等於零，α_1 就等於無窮大而我們得到等式 $\alpha=q_1$．除了這種特殊情況，它和我們化無理數成連分數是不相干的，我們可以肯定 α_1 是大於 1 的正數，對於這個數 α_1，我們和對於 α 一樣地來處理，而寫成等式

$$\alpha_1=q_2+\frac{1}{\alpha_2},\quad q_2=[\alpha_1],\quad \frac{1}{\alpha_2}=\{\alpha_1\}.$$

繼續這個步驟，我們得到一系列等式：

$$\left.\begin{array}{ll}\alpha=q_1+\dfrac{1}{\alpha_1}, & q_1=[\alpha],\\ \alpha_1=q_2+\dfrac{1}{\alpha_2}, & q_2=[\alpha_1],\\ \alpha_2=q_3+\dfrac{1}{\alpha_3}, & q_3=[\alpha_2],\\ \cdots\cdots\cdots\cdots & \\ \alpha_{n-1}=q_n+\dfrac{1}{\alpha_n}, & q_n=[\alpha_{n-1}],\\ \cdots\cdots\cdots\cdots & \end{array}\right\} \tag{54}$$

這樣逐個地構成整數數列 $q_1, q_2, q_3, \cdots\cdots, q_n, \cdots\cdots$ 當 α 是有理數，換句話說，當 $\alpha=\frac{a}{b}$，而 a 和 b 是正整數的時候，不難看出，就結果本身說，和用歐幾里得算法來求部分商的步驟並無不同〔參看公式(6)〕. 所以，當 α 是有理數的時候，它應當是有止境的. 當 α 是無理數的時候，這個數列必是無止境的. 實際上，若在某一個整數 n 時，α_n 是整數，則由此可得 α_{n-1} 必是有理數，這也就引出 α_{n-2} 也是有理數，這樣下去，最後，α_1 是有理數. 從公式(54)，作一連串的代入把 $\alpha_1, \alpha_2, \cdots\cdots, \alpha_{n-1}$ 消去，我們得到連分數

$$\alpha=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cdots+\cfrac{1}{q_n+\cfrac{1}{\alpha_n}}}}, \qquad (55)$$

因爲 n 可以取得任意的大，這個分數可以改寫成無限連分數的形式

$$\alpha=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cdots+\cfrac{1}{q_n+\cdots}}}.$$

恰如我們在前面第四節已經說過的一樣，近似分數間的關係(8)在這種情況中也保存着，因爲它無關於連分數的有限或無限. 從這個關係(8)，和我們已經見到的一樣，對於偶數項的近似分數可得到不等式(25). 這個不等式(25)將又再作

爲證明方程式(51)存在有解的根據，但這證明本身比起 $A=2$ 的特殊情況來要複雜得多.

〔定理 3〕 **當 A 是任意正整數而 $\sqrt{A}$ 是無理數的時候，方程式 (51)**

$$x^2-Ay^2=1$$

具有非常解 $[x_0, y_0]$ $x_0>0$ $y_0>0$.

〔證明〕 由於方程式 (51) 解的存在的證明相當複雜，我們分這個證明成若干步. 第一步，是證明存在着一個正整數 k，它具有這樣的性質，使得方程式

$$x^2-Ay^2=k \qquad (56)$$

必具有無限多組正整數解 x 和 y. 實際上，我們研究二項式 x^2-Ay^2，用無理數 $\alpha=\sqrt{A}$ 的偶數項近似分數的分子和分母代替 x^2-Ay^2 中的 x 和 y，則

$$z_{2n}=P_{2n}^2-AQ_{2n}^2=(P_{2n}-\alpha Q_{2n})(P_{2n}+\alpha Q_{2n}). \qquad (57)$$

但從

$$0<P_{2n}-\alpha Q_{2n}<\frac{1}{Q_{2n+1}},$$

立刻得出：

$$0<P_{2n}+\alpha Q_{2n}=2\alpha Q_{2n}+P_{2n}-\alpha Q_{2n}<2\alpha Q_{2n}+\frac{1}{Q_{2n+1}}.$$

我們現在運用這末了的兩個不等式去估計 z_{2n}. 用這些不等式中的最大的值代替等式 (57) 右邊的兩個因式，對於 z_{2n} 我們得到不等式

$$0<z_{2n}<\frac{1}{Q_{2n+1}}\left(2\alpha Q_{2n}+\frac{1}{Q_{2n+1}}\right)<2\alpha+1, \qquad (58)$$

因爲 Q_{2n} 小於 Q_{2n+1}. 相應地用 P_{2n} 和 Q_{2n} 代替二項式

$$z=x^2-Ay^2$$

中的 x 和 y 則 z 取正整數值。由此，所有的數 z_2 z_4, ……, z_{2n}, ……都必是不超過同一個數 $2\alpha+1$ 的正整數。但因爲 $\alpha=\sqrt{A}$ 是一個無理數，則這連分數是無限的，也就是說，這樣的數對 P_{2n} 和 Q_{2n} 是無限多的。在正整數 z_2 z_4 ……, z_{2n}, ……中就不同，它們只是有限的，因爲它們是在 1 和一個與 n 無關的定數 $2\alpha+1$ 之間，所以至多只能有 $[2\alpha+1]$ 個整數。換句話說，無限數列 z_2 z_4, ……, z_{2n}, ……並不是別的，只是整數 1,2,3,……, $[2\alpha+1]$ 依某種形式重複所得的數列，並且所有這些數還不必一定都在我們的數列 z_2, z_4, ……, z_{2n}……當中出現。因爲數列 z_2, z_4, ……, z_{2n}, ……是無限的，而它們中相異的數值又是有限的，所以至少一個數 k $(1\leqslant k\leqslant[2\alpha+1])$ 在這個數列中重複無限多次。換句話說，在數對 $[P_2, Q_2]$ $[P_4, Q_4]$, ……, $[P_{2n}, Q_{2n}]$, ……中有無限多這樣的數對，將它們代替 $z=x^2-Ay^2$ 的 x 和 y，則它們卽取同一數值 k。由此，我們已證明了，存在着正整數 k，對於它，方程式 (56) 具有無限多的正整數解 x 和 y。對於所給的 k，我們重新編定這些作爲方程式 (56) 的解的數對的數碼，並且用 $[u_1, v_1]$, $[u_2, v_2]$, ……, $[u_n, v_n]$, ……來表示它們，則我們可得到，

$$u_n^2-Av_n^2=k. \qquad (57)$$

我們注意，數對列 $[u_1, v_1]$, $[u_2, v_2]$, ……, $[u_n, v_n]$, ……必是 α 的偶數項近似分數的分子和分母數對列的一部分。若我們能夠確定 $k=1$，那末我們已經證明方程式 (51) 具有無限多的正整數解。因爲我們不能夠確定這一點，就姑且假定 $k>1$（反過來，當 $k=1$ 的時候，一切都已證明了），而轉到我們證

明的第二步．現在證明,在整數對$[u_1, v_1]$, ……$[u_n, v_n]$, ……中必有無限多的數對,在除以數 k 的時候,得出同樣的餘數,——換句話說,存在着這樣的兩個小於 k 的正整數 p 和 q,使得對於無限多的數對$[u_1, v_1]$,$[u_2, v_2]$, ……$[u_n, v_n]$……有等式

$$u_n = a_n k + p, \quad v_n = b_n k + q. \tag{60}$$

這兒 a_n 和 b_n 是 u_n 和 v_n 除以 k 所得的商,而 p 和 q 是餘數．實際上,若我們用整數 k 來除 u_n 和 v_n, $k>1$ 則我們即得到關係(60),這兒除得的餘數,總是在零和 $k-1$ 之間． 因為用 k 除數 u_n 所得的餘數只能是 $0,1,2,\cdots\cdots, k-1$,完全一樣,用 k 除數 v_n 所得的餘數也只能是 $0,1,2,\cdots\cdots, k-1$;所以,當用 k 去除兩個數 u_n 和 v_n 的時候,可能有的餘數對必是 $k \cdot k = k^2$ 個．這也顯然可從下面的事實看出來,即每對數$[u_n, v_n]$相應地有一個餘數對$[p_n, q_n]$,各個 p_n 和 q_n 都不能取大於 k 的不同數值,而數對因此必不超過 k^2 個．由此可知,每對整數$[u_n, v_n]$,當除以 k 的時候,相應地有一個餘數對$[p_n, q_n]$．但各餘數對的個數是有限的,不會超過 k^2 個的,而數對$[u_n, v_n]$是無限的．這就是說,因為在數對列$[p_1, q_1]$,$[p_2, q_2]$, ……,$[p_n, q_n]$, ……中只具有有限個不同的數對,所以至少有一對重複無限多次．用$[p, q]$表示這個餘數對,我們得到,適合等式(60)的數對$[u_n, v_n]$有無限多．因為我們剛才證明,有某種確定的值 p 和 q 存在,不是一切數對$[u_n, v_n]$都適合於等式(60),我們可以重新編排適合於等式(60)的一切數對$[u_n, v_n]$,而用$[R_n, S_n]$來表示．由此,無限數對列

$[R_1, S_1]$, $[R_2, S_2]$, ……, $[R_n, S_n]$……是數對列$[u_n, v_n]$的一部分，而$[u_n, v_n]$又是數α的偶數項近似分數的分子和分母數對列的一部分. 這一列的數對適合於方程式(59)，並且當除以k的時候得出同一的餘數p和q.

現在，在我們已確定了存在着無限多這樣的正整數對R_n和S_n以後，我們就可以轉到我們證明的第三步，即最後一步.

首先，我們注意，數對$[R_n, S_n]$既然是近似分數的分子和分母的數對，就應當是互質數對，即各對數都沒有公因數，實際上，若在關係式(24)中，用$2k$代替k，而設

$$\delta_{2k}=\frac{P_{2k}}{Q_{2k}}, \quad \delta_{2k-1}=\frac{P_{2k-1}}{Q_{2k-1}},$$

則從等式

$$\frac{P_{2k}}{Q_{2k}}-\frac{P_{2k-1}}{Q_{2k-1}}=\frac{1}{Q_{2k}Q_{2k-1}},$$

兩邊乘以$Q_{2k}Q_{2k-1}$，我們得到等式

$$P_{2k}Q_{2k-1}-Q_{2k}P_{2k-1}=1. \qquad (61)$$

整數P_{2k}, Q_{2k}, P_{2k-1}, Q_{2k-1}中間的這一關係表明，若P_{2k}和Q_{2k}具有大於1的公因數，則它的左邊各項應當被這個公因數除得盡. 但在等式的右邊是1，它不能被任何大於1的整數所整除. 這樣一來，R_n和S_n是互質的；它們只能是近似分數的分子和分母，就確定了. 由關係(7)，立刻也得到，

$$Q_2<Q_4<\cdots\cdots<Q_{2n}<\cdots\cdots.$$

從R_n和S_n的互質，以及從互不相同的數Q_{2n}所成數列中取出的數$S_1, S_2, \cdots\cdots, S_n, \cdots\cdots$也是各不相同的，立刻可以推出，在無限分數列

$$\frac{R_1}{S_1}, \quad \frac{R_2}{S_2}, \cdots\cdots, \frac{R_n}{S_n}, \cdots\cdots$$

中沒有相同的數. 依照數 R_n 和 S_n 的定義,我們寫出下面的兩個等式:

$$R_1^2-AS_1^2=(R_1-aS_1)(R_1+aS_1)=k \qquad (62)$$

和

$$R_2^2-AS_2^2=(R_2-aS_2)(R_2+aS_2)=k, \qquad (63)$$

這兒仍然是 $a=\sqrt{A}$.

再,因爲 $a^2=A$,我們有:

$$(R_1-aS_1)(R_2+aS_2)$$
$$=R_1R_2-AS_1S_2+a(R_1S_2-S_1R_2), \qquad (64)$$

並且完全一樣

$$(R_1+aS_1)(R_2-aS_2)$$
$$=R_1R_2-AS_1S_2-a(R_1S_2-S_1R_2). \qquad (65)$$

但 R_n 和 S_n 當除以 k 時,具有同一個與 n 無關的餘數. 因而由關係(60),

$$R_n=c_nk+p, \quad S_n=d_nk+q. \qquad (66)$$

由此,用一些改變和代入的方法,我們就得到等式:

$$R_1R_2-AS_1S_2=R_1(c_2k+p)-AS_1(d_2k+q)$$
$$=R_1[(c_2-c_1)k+c_1k+p]-AS_1[(d_2-d_1)k+d_1k+q]$$
$$=R_1[(c_2-c_1)k+R_1]-AS_1[(d_2-d_1)k+S_1]$$
$$=k[R_1(c_2-c_1)-AS_1(d_2-d_1)]+R_1^2-AS_1^2$$
$$=k[R_1(c_2-c_1)-AS_1(d_2-d_1)+1]=kx_1, \qquad (67)$$

這兒 x_1 是一個整數,又,因爲 $R_1^2-AS_1^2=k$. 完全一樣的,

$$R_1S_2-S_1R_2=R_1[(d_2-d_1)k+d_1k+q]$$
$$-S_1[(c_2-c_1)k+c_1k+p]$$

$$=R_1[(d_2-d_1)k+S_1]-S_1[(c_2-c_1)k+R_1]$$
$$=k[R_1(d_2-d_1)-S_1(c_2-c_1)]=ky_1, \qquad (68)$$

這兒 y_1 也是個整數．我們可以肯定 y_1 不等於零．實際上，若 $y_1=0$，則

$$ky_1=R_1S_2-R_2S_1=0,$$

由此

$$\frac{R_1}{S_1}=\frac{R_2}{S_2}.$$

這末了的一個等式是不可能的，因爲我們已經證明所有的分數 $\frac{R_n}{S_n}$ 是各各不同的．等式(64)和(65)表明，

$$(R_1-\alpha S_1)(R_2+\alpha S_2)=kx_1+\alpha ky_1$$
$$=k(x_1+\alpha y_1) \qquad (69)$$

和

$$(R_1+\alpha S_1)(R_2-\alpha S_2)=kx_1-\alpha ky_1$$
$$=k(x_1-\alpha y_1). \qquad (70)$$

現在把等式(62)和(63)邊邊相乘並且利用等式(69)和(70)，我們得：

$$k^2=(R_1^2-AS_1^2)(R_2^2-AS_2^2)$$
$$=(R_1-\alpha S_1)(R_2+\alpha S_2)(R_1+\alpha S_1)(R_2-\alpha S_2)$$
$$=k^2(x_1+\alpha y_1)(x_1-\alpha y_1)$$
$$=k^2(x_1^2-Ay_1^2). \qquad (71)$$

消去k^2，最後得到：

$$x_1^2-Ay_1^2=1. \qquad (72)$$

但 y_1 不等於零，可知 x_1 也不能是零．否則等式的左邊是一個負數而右邊是 1 是不可能的． 由此，即使假定 k 不等於 1，我們也求得了適合於方程式 (51) 的不等於零的兩個整數 x_1

和y_1. 這就完全完成了類型(51)方程式的討論，因爲我們知道了，當A是整數，$A>0$，而$\sqrt{A}$是無理數的時候，這樣的方程式總具有解；而藉助於已經證明存在的最小解，我們就能夠求出它的一切解.

實際上，最小解是可以由選擇x_0和y_0的方法求出來的.

這樣一來，我們已經完全研究了，在方程式

$$x^2-Ay^2=1$$

中，$A>0$而$\alpha=\sqrt{A}$是無理數的情形了.

若$A>0$而$\alpha=\sqrt{A}$是整數，則這個方程式可以改寫成

$$x^2-\alpha^2y^2=(x+\alpha y)(x-\alpha y)=1,$$

並且因爲α是一個整數，所以若x_0和y_0是適合於它的整數，等式

$$x_0+\alpha y_0=1,\quad x_0-\alpha y_0=1$$

或等式

$$x_0+\alpha y_0=-1,\quad x_0-\alpha y_0=-1,$$

就必有一組成立。因爲兩個整數的積，只有在它們兩個數同時等於$+1$或-1的時候，才能夠等於1。這兩組具有未知數x_0和y_0的二元聯立方程式只有兩組常解：$x_0=1,y_0=0$；$x_0=-1,y_0=0$. 由此，**方程式(51)當A等於一個整數的平方的時候，只具有整數的常解$x_0=\pm1,y_0=0$. 當A是負整數的時候，方程式(51)也同樣只具有整數的常解**(當$A=-1$的時候，有和上述對稱的兩組常解$x_0=0$，$y_0=\pm1$適合於方程式).

現在我們來研究更一般情況的方程式

$$x^2-Ay^2=C,\tag{73}$$

這兒，A 是大於零的整數，C 是整數；$\alpha=\sqrt{A}$ 是無理數．我們已經見到，當 $C=1$ 的時候，這個方程式總具有無限多組的整數解 x 和 y．當 C 和 A 是任意整數的時候，這樣的方程式一般地不能有整數解．

〔範例〕 證明方程式

$$x^2-3y^2=-1 \qquad (74)$$

一般地沒有整數解 x 和 y．首先，我們注意，奇數的平方數，在除以 8 的時候，總得到餘數 1．實際上，因為一切的奇數 a 可以寫成這種形式 $a=2N+1$，這兒 N 是整數，而

$$a^2=(2N+1)^2=4N^2+4N+1=4N(N+1)+1$$
$$=8M+1, \qquad (75)$$

因為 N 和 $N+1$ 裏面必有一個是偶數，這兒 M 是整數．又，若 $[x_0\ y_0]$ 是方程式(74)的解，則 x_0 和 y_0 不能同是偶數．若 x_0 和 y_0 同是偶數或奇數，則 $x_0^2-3y_0^2$ 必定是偶數而不能夠等於 1．又若 x_0 是奇數而 y_0 是偶數，則當 x_0^2 除以 4 的時候，得着餘數 1，$-3y_0^2$ 是能夠被 4 除盡的，而 $x_0^2-3y_0^2$ 當除以 4 的時候餘數却是 1．這是不可能的，因為右邊除以 4 的時候，一般地總得到餘數 -1 或 $3=4-1$．末了，若 x_0 是偶數，而 y_0 是奇數，則 x_0^2 能夠被 4 除盡，而 $-3y_0^2$ 根據(75)可以寫成這樣的形式

$$-3y_0^2=-3(8M+1)=-24M-3=4(-6M-1)+1,$$

也就是，在除以4的時候，得到餘數1．因而，$x_0^2-3y_0^2$ 在除以 4的時候，應當仍然得到餘數 1，這正和我們已經見到過一樣是不可能的．因此，能夠適合於方程式(74)的整數 x_0 和 y_0 不存在．

我們不停留在這個問題上面，這就是 C 和 A 處在怎樣的情況，方程式 (73) 將具有整數解的問題，——這個困難問題我們可以藉助代數學中數論的一般無理方根的定理來解決，——我們來研究在方程式(73)具有非常解的這種情況．這個非常解我們叫做 $[x', y']$，若 $x', y' \neq 0$．由此，設方程式 (73) 具有非常解 $[x', y']$；換句話說，設

$$x'^2 - Ay'^2 = C. \qquad (76)$$

由同樣的 A 我們來研究方程式

$$x^2 - Ay^2 = 1. \qquad (77)$$

在 $A>0$ 和 $\alpha = \sqrt{A}$ 是無理數的時候，這個方程式具有無限多的正整數解，而任何這樣的解 $[\bar{x}, \bar{y}]$ 必是：

$$\bar{x} = \pm x_n, \quad \bar{y} = \pm y_n,$$

這兒 x_n 和 y_n 依照公式(50)決定．因為 $[\bar{x}, \bar{y}]$ 是方程式 (77) 的解，所以

$$\bar{x}^2 - A\bar{y}^2 = (\bar{x} + \alpha\bar{y})(\bar{x} - \alpha\bar{y}) = 1.$$

等式(76)就它自己一方面說可以寫成這樣形式，

$$(x' + \alpha y')(x' - \alpha y') = C.$$

這最後的兩個等式邊邊相乘，我們得：

$$(x' + \alpha y')(\bar{x} + \alpha\bar{y})(x' - \alpha y')(\bar{x} - \alpha\bar{y}) = C. \qquad (78)$$

但 $$(x' + \alpha y')(\bar{x} + \alpha\bar{y}) = x'\bar{x} + Ay'\bar{y} + \alpha(x'\bar{y} + y'\bar{x})$$

而相應地，同樣

$$(x' - \alpha y')(\bar{x} - \alpha\bar{y}) = x'\bar{x} + Ay'\bar{y} - \alpha(x'\bar{y} + y'\bar{x}).$$

利用這兩個等式，我們可以把等式(78)寫成這種形式

$$[x'\bar{x} + Ay'\bar{y} + \alpha(x'\bar{y} + y'\bar{x})][x'\bar{x} + Ay'\bar{y} - \alpha(x'\bar{y} + y'\bar{x})] = C$$

或成這種形式

$$(x'\bar{x}+Ay'\bar{y})^2-A(x'\bar{y}+y'\bar{x})^2=C.$$

這樣我們就證明了，若 $[x',y']$ 是方程式 (73) 的解，則這個方程式也為這對數 $[x,y]$ 所適合：

$$x=x'\bar{x}+Ay'\bar{y},\quad y=x'\bar{y}+y'\bar{x},\tag{79}$$

這兒 $[\bar{x},\bar{y}]$ 是方程式 (77) 的任意的整數解. 這樣一來，我們證明了，**若方程式(73)至少具有任何一組解，則它就具有無限多的解.**

自然，不能就肯定，公式 (79) 給出了方程式 (73) 的一切解. 在代數數論中，證明了在取方程式(73)的一定組數(這數目是由 A 和 C 來決定的)的解，並且藉助於公式 (79) 把它們擴充以後，則這方程式的一切解都可以得到. 方程式 (73) 在 A 是負的或等於整數平方的時候，只能具有有限組數的整數解. 這個簡單地就可以證明的命題，我們留給讀者來證明.

這種最一般形式

$$Ax^2+Bxy+Cy^2+Dx+Ey+F=0\tag{80}$$

的二元二次方程式，這兒 A,B,C,D,E 和 F 都是整數，它的整數解可以用變換方法歸到解(73)型方程式裏，其中 A 或為正或為負. 因此，若存在有解，則這些解的變化和性質就和 (73) 型方程式的一樣. 綜合前面所講的一切，我們現在可以說，**(80) 型的二元二次方程式，可以不具有整數解，可以只具有有限組數整數解；末了，也可以具有無限多組這樣的解，並且這些解可以從有限多個由公式(79)所給的廣義幾何級數中取出來.** 試將二元二次方程式的整數解的變化和性質跟一次

方程式的相比較，我們可以明確一個非常重要的情況．就是，一次方程式的整數解，它們存在的時候，就構成一個算術級數；而二次方程式的解，它們是無限多組的時候，就可從有限多組廣義幾何級數中取出．換句話說，在二次方程式的情形，可以是方程式的解的整數對，比較起可以是一次方程式的解的整數對來就難遇到得多．這個情況，並不是偶然的．原來，高於二次的二元方程式，一般地說，只可以具有有限組數的整數解．這個法則例外極少．

六 高於二次的二元方程式

高於二次的二元方程式，除了少數例外，幾乎總是只能有有限組數整數解 x 和 y．首先，我們來研究方程式

$$a_0x^n+a_1x^{n-1}y+a_2x^{n-2}y^2+\cdots\cdots+a_ny^n=c, \qquad (81)$$

這兒 n 是大於 2 的整數，而所有的數 a_0、a_1、a_2、……，a_n、c 都是整數．

正如在二十世紀初年，屠耶證明了的，這樣的方程式只具有有限組數的整數解 x 和 y，除了例外情形，即在這個方程式左邊是一次二項齊次式的乘方，或二次三項齊次式的乘方．在後一種情形，我們的方程式必具有這兩種形式

$$(ax+by)^n=c_0, \quad (ax^2+bxy+cy^2)^n=c_0$$

中的一種，而因此就歸到一次或二次方程式，因為要它有整數解存在，c_0 必須是整數的 n 次方．由於屠耶的方法相當複雜，我們這裏不能對它加以敘述，我們只作一些解釋性的注解，這些注解能夠對方程式(81)的解是有限的這個事實，作本質上

的說明㊀.

以 y^n 除方程式(81)的兩邊，我們的方程式於是成爲這樣形式，

$$a_0\left(\frac{x}{y}\right)^n+a_1\left(\frac{x}{y}\right)^{n-1}+\cdots\cdots+a_{n-1}\frac{x}{y}+a_n=\frac{c}{y^n}. \qquad (82)$$

爲了說明簡單些，我們假定不僅方程式

$$a_0z^n+a_1z^{n-1}+\cdots\cdots+a_{n-1}z+a_n=0 \qquad (83)$$

的一切根不相同，以及 $a_0a_n\neq0$，並且還假定這個方程式的根不能是較低次的整數係數方程式的根．對我們的問題來說，這種情形才是根本的．

在高等代數中，證明了一切代數方程式至少具有一個根，於是，基於這種事實，還極簡單地證明了，若 α 是一個多項式的根，則整個多項式可以被 $z-\alpha$ 整除，由此我們得到表示多項式成乘積的形式

$$a_0z^n+a_1z^{n-1}+\cdots\cdots+a_n=a_0(z-\alpha_1)(z-\alpha_2)\cdots\cdots(z-\alpha_n), \quad (84)$$

這兒 $\alpha_1,\alpha_2,\cdots\cdots,\alpha_n$ 是所給的多項式的 n 個根．利用把多項式表示成乘積形式的公式，我們可以把方程式(82)改寫成這種形式，

$$a_0\left(\frac{x}{y}-\alpha_1\right)\left(\frac{x}{y}-\alpha_2\right)\cdots\cdots\left(\frac{x}{y}-\alpha_n\right)=\frac{c}{y^n}. \qquad (85)$$

我們假定方程式(85)有着無限多組的整數解 $[x_k,y_k]$．就是說，存在着 y_k 具有任意大的絕對值的解．若存在着無限多組數對，y_k 是有界限的，在絕對值上小於某一個定數，而 x_k 則任意大，那末對於這樣的 x_k，左邊是任意大而右邊則仍爲

㊀ 對於這一個問題的文獻，收集在，例如蓋里馮德的論文‘超越數論及利用代數數來逼近代數數’，‘數學成就’4卷4期(32)，1949，第19頁．

有限，這是不可能的。設 y_k 很大，則方程式 (85) 的右邊將很小，也就是左邊也應當很小。但方程式的左邊是含有 $\frac{x_k}{y_k}$ 的 n 個因子的積，而 a_0，因爲它是整數，所以不會小於 1。就是說，左邊的微小只能由某些在絕對值上很小的差數

$$\frac{x_k}{y_k}-\alpha_m$$

來決定。顯然，這差只能在 α_m 是實數時才會很小，換句話說，就是在不具有等式 $\alpha_m=a+bi$，$b\neq0$ 的場合才會很小。否則，因爲

$$\left|\frac{x_k}{y_k}-a-bi\right|=\sqrt{\left(\frac{x_k}{y_k}-a\right)^2+b^2}>|b|,$$

我們的差數的絕對值就不能任意小。方程式(85)左邊的兩個因子，這兩個差，就絕對值來說，不能是同時很小，因爲由於數 α_m 是各不相同的，

$$\left|\left(\frac{x_k}{y_k}-\alpha_m\right)-\left(\frac{x_k}{y_k}-\alpha_s\right)\right|=\left|\alpha_m-\alpha_s\right|\neq0. \qquad (86)$$

若一個差的絕對值小於 $\frac{1}{2}\left|\alpha_m-\alpha_s\right|$，則由(86)，另一個差就應當大於 $\frac{1}{2}\left|\alpha_m-\alpha_s\right|$，這是由於和的絕對值不大於絕對值的和。因爲所有的 α_m 是不相同的，所以就絕對值來說，最小的差數 $\left|\alpha_m-\alpha_s\right|$ 也必大於零($m\neq s$)。用 $2d$ 表示這個值，我們就得，對於每個充分大的 y_k，因爲 y_k 無限地增長，必有

$$\left|\frac{x_k}{y_k}-\alpha_m\right|<d,$$

而

$$\left|\frac{x_k}{y_k}-\alpha_s\right|>d, \quad s=1,2,\cdots\cdots,n, \quad s\neq m. \qquad (87)$$

於是，因爲積的絕對值等於絕對值的積，從方程式 (85) 我們就得

$$|a_0|\left|\frac{x_k}{y_k}-\alpha_1\right|\cdots\cdots\left|\frac{x_k}{y_k}-\alpha_{m-1}\right|\left|\frac{x_k}{y_k}-\alpha_m\right|\left|\frac{x_k}{y_k}-\alpha_{m+1}\right|$$
$$\cdots\cdots\left|\frac{x_k}{y_k}-\alpha_n\right|=\frac{|c|}{|y_k|^n}. \qquad (88)$$

但若在等式裏面，每一個差數 $\left|\frac{x_k}{y_k}-\alpha_s\right|$，$s\neq m$ 都用較小的值 d 去代替而用 1 代替 $|a_0|$，因爲小於 1 的整數 $|a_0|$ 是沒有的．那末(88)的左邊就變得小於右邊，而我們得到不等式

$$d^{n-1}\left|\frac{x_k}{y_k}-\alpha_m\right|<\frac{|c|}{|y_k|^n},$$

或不等式

$$\left|\frac{x_k}{y_k}-\alpha_m\right|<\frac{c_1}{|y_k|^n},\ c_1=\frac{|c|}{d^{n-1}}, \qquad (89)$$

這兒 c_1 跟 x_n 和 y_n 無關，α_m 的數目不超過 n，而對於任何 m，數對中必須適合不等式 (89) 的數對 $[x_k,y_k]$ 是無限多的．因此，存在着這樣的定數 m，使得對於相應的 α_m，不等式(89)無限多次成立．換句話說，若方程式(81)具有無限多的整數解，則整數係數的代數方程式 (83) 具有這樣的根 α，使得有任意大的 q，使不等式

$$\left|\alpha-\frac{p}{q}\right|<\frac{A}{q^n}, \qquad (90)$$

成立，這兒 A 是跟 p 和 q 無關的常數，p 和 q 是整數，而 n 是 α 所滿足的方程式的次數． 若 α 是任意的實數，則它可能這樣挑選，使得不等式 (90) 實際存在着無限多的整數解 p 和 q．但在我們的情況下，α 是整數係數代數方程式的根． 這樣的數叫做代數數，它具有特殊的性質． 這個數所適合的最低次整數係數代數方程式的次數叫做這個代數數的次數．

　　屠耶證明了，對於 n 次代數數 α，不等式

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^{\frac{n}{2}+1}},\quad n\geqslant 3, \tag{91}$$

只能具有有限多組整數解 p 和 q. 但若 $n\geqslant 3$,不等式(90)的右邊當 q 適當大的時候,比不等式(91)的右邊小,因爲 $n>\frac{n}{2}+1$. 因此,若不等式(91)只能具有有限多組整數解 p 和 q,則不等式(90)也應當只具有有限組數的解. 就是說,方程式(81)只能具有有限組數的整數解,只要方程式(83)的一切根不能是低於 n 次的整數係數方程式的根的時候. 當 $n=2$ 的時候,我們容易證明,不等式(90)實際上,對於某些數 A,能夠具有無限多組的整數解 p 和 q. 屠耶的定理到後來被大大地充實了. 必須注意,他的定理的證明方法原則上並不能使我們求出解的值的上界.——換句話說,即依照係數 a_0 a_1 a_2, ……, a_n 和 c, $|x|$ 和 $|y|$ 可能有的值的界限. 這個問題今天還等待解決. 屠耶的方法雖不能使我們求出解的值的界限,却能使我們求出方程式(83)的解的數目的界限,這誠然是十分粗糙的. 對於(83)型的個別方程式,這個界限可能相當精確. 例如,蘇聯數學家吉羅涅(Б. Н. Делоне)證明了㊀,方程式

$$ax^3+y^3=1$$

對於整數 a,除了常解 $x=0, y=1$ 外,不能再具有一組以上的整數解 x 和 y. 此外,他還證明了,方程式

$$ax^3+bx^2y+cxy^2+dy^3=1,$$

㊀ 對於這個問題的文獻,參看1948年國立技術理論書籍出版社出版的'蘇聯數學三十年'中蓋里馮德的論文'數論'.

當 a,b,c 和 d 是整數的時候，不能具有五組以上的整數解 x 和 y.

設 $P(x,y)$ 是關於 x 和 y 任意的整數係數多項式，換句話說，

$$P(x,y)=\sum A_{ks}x^k y^s,$$

這兒 A_{ks} 是整數. 若它不能表成另外兩個整數係數多項式的積，這兩個整數係數多項式沒有一個只是一個數目的，我們就說這樣的多項式是既約的.

用特殊而且很複雜的方法，齊蓋里 (К. Зигель) 證明了，方程式

$$P(x,y)=0,$$

這兒 $P(x,y)$ 是關於 x 和 y 的高於二次的既約多項式(換句話說，在它裏面含的是這種形式 $A_{ks}x^k y^s$ 的項，這兒 $k+s>2$)，具有無限多的整數解 x 和 y 的充分而且必要的條件是，存在着這樣的數 $a_n, a_{n-1}, \cdots\cdots, a_0, a_{-1}, a\cdots\cdots, a_{-n}$ 和 $b_n, b_{n-1}, \cdots\cdots, b_0, b_{-1}, \cdots\cdots, b_{-n}$，使得在上面的方程式中，用

$$x=a_n t^n+a_{n-1}t^{n-1}+\cdots\cdots+a_0+\frac{a_{-1}}{t}+\cdots\cdots+\frac{a_{-n}}{t^n},$$

$$y=b_n t^n+b_{n-1}t^{n-1}+\cdots\cdots+b_0+\frac{b_{-1}}{t}+\cdots\cdots+\frac{b_{-n}}{t^n}$$

去代替 x 和 y，我們得到關於 t 的恆等式

$$P(x,y)\equiv 0,$$

這裏 n 是某一個整數.

七　高於二次的三元代數方程式和某些指數方程式

若是說，對於二元方程式我們能夠回答，關於存在有限或無限組整數解的問題；那末，對於具有兩個以上未知數並且高於二次的方程式，在這個問題上，我們只能對於極特殊的一類方程式給與回答。但是，在後一種情況中，是可以解決異常困難的關於確定方程式的一切整數解的問題的。我們用所謂大飛馬定理來作例子。

著名的法國數學家比爾·飛馬曾經說過這樣的論斷，即方程式

$$x^n+y^n=z^n \qquad (92)$$

在整數 $n\geqslant3$ 的時候，沒有正整數解 x,y,z（除了 $xyz=0$ 這種正整數的 x,y,z）。儘管飛馬肯定說，他具有這一論斷的證明（大概用的遞降法，關於這點下面將要談到），但它的證明後來並沒有找到。不僅這樣，當數學家古米耳試圖去求這一個證明，並且甚至於在一個時期他以爲已經找到了證明，他發現了一個命題，這在通常整數範圍裏是正確的，但在對於研究飛馬問題時所必須遇到的某種比較複雜的數組却是不正確的。這種情況，是由於所謂**代數整數**——換句話說，即帶有有理整數係數而且最高次項係數等於 1 的代數方程式的根——不能用唯一的方法分解成質因數，也就是不可能分解成有同一代數性的整因子。而通常的整數却以唯一的方法分解成質因數。例如，$6=2\cdot3$ 在通常的整數集裏就不能有別的分解法。我們

來研究這樣形式 $m+n\sqrt{-5}$ 的一切代數整數的集，這兒 m 和 n 是通常的整數．容易看出，兩個這樣的數的和跟積仍然是整數集裏的數．一個數集，若它具有這樣的性質，即它包含屬於它的任何兩數的和跟積，就叫它做一個環．依照這個定義，數 $2,3,1+\sqrt{-5},1-\sqrt{-5}$ 就包含在我們的環裏．在這環中，這些數我們都能夠容易地確定它是質數，就是說，不能被表示成我們環中兩個不等於么元(單位)的整數的積．但

$$6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5});$$

換句話說，數 6 在我們的環裏，被分成質因數的方法不是唯一的．同樣的現象，即質因數分解的非唯一性也在別的更複雜的代數整數環裏可能發生．在發現了這種現象之後，古米耳已經相信他關於一般情況的大飛馬問題的證明是不對的．爲了克服非唯一性的困難，古米耳建立了理想數論．這種理論現在在代數學和數論中起着非常巨大的作用．但即或借助於這個新的理論，古米耳也不能完全地證明大飛馬定理，他只就那種至少能被一個所謂正規質數除盡的 n，證明了這一定理．我們不來解釋正規質數的概念，我們只能夠指出，直到現在爲止，還不知道這樣的質數的數目，是存在着有限多或無限多．

在現代，大飛馬定理對於許多的 n，特別是對於能夠被小於 100 的質數所整除的 n，已經證明成立了．大飛馬定理，由於要想去證明它而發現了理想數論，在數學的發展上起了巨大的作用．但是，同時應當指出，用完全不同的方法和按照不同的動機，這一個理論曾經被在自己的科學活動最盛時期死

去的著名俄國數學家左洛達略夫 (Е. И. Золотарёв) 建立了起來. 大飛馬定理的證明，特別是建立在數的整除性的考慮上的論證，只不過具有遊戲的趣味罷了. 當然，若這證明是用新的和有效的方法得到的，那末，它的價值，即和方法自身相聯系着的價值可能是很大的. 應當指出，在我們的時代數學的愛好者們要想用完全初等的方法去證明飛馬定理注定了不會成功的. 依靠數的整除性理論的初等論證，古米耳早已做過了，並且非常優秀的數學家們更進一步地研究，絲毫也沒有得到結果.

我們這裏舉出在 $n=4$ 時，飛馬定理的證明，因爲構成這個證明的遞降法是很有趣味的.

〔定理 4〕 **飛馬方程式**

$$x^4+y^4=z^4 \tag{93}$$

沒有 $xyz\neq 0$ 的整數解 x,y,z.

〔證明〕 我們來證明一個更有力的定理，即方程式

$$x^4+y^4=z^2 \tag{94}$$

沒有 $xyz\neq 0$ 的整數解 x,y,z. 從這個定理已可立刻得出方程式 (93) 缺少整數解. 若方程式 (94) 具有異於零的整數解 x,y,z，那末，可以假定這些數是兩兩互質的. 實際上，若有一個解其中的 x 和 y 具有最大公因數 $d>1$，則

$$x=dx_1,\quad y=dy_1,$$

這兒 $(x_1,y_1)=1$. 以 d^4 除方程式(94)的兩邊，我們將有

$$x_1^4+y_1^4=\left(\frac{z}{d^2}\right)^2=z_1^2. \tag{95}$$

但 x_1 和 y_1 是整數，就是說 $z_1=\frac{z}{d_2}$ 也是整數．若 z_1 和 y_1 有公因數 $k>1$，則由 (95) x_1^2 應當能夠被 k 除得盡，也就是說，x_1 和 k 不能是互質數．這樣一來，我們已證明了，若方程式 (94) 存在着異於零的整數解，則同樣地存在着異於零並且互質的整數解．因此我們只須證明，方程式(94)不具有異於零並且兩兩互質的整數解．在下面的證明過程中，說到方程式 (94) 具有解，我們就假定，它是具有正的並且兩兩互質的整數解．

在第 3 節我們已經證明，方程式(12)

$$x^2+y^2=z^2 \tag{96}$$

的一切正整數解，是兩兩互質而由公式(18)所決定的，並且具有這樣的形式

$$x=uv,\quad y=\frac{u^2-v^2}{2},\quad z=\frac{u^2+v^2}{2}, \tag{97}$$

這兒 u 和 v 是任意兩個正的互質的奇數．

我們將增加公式 (97) 的另一種式子，即決定方程式 (96) 的一切解的另一種式子．因為 u 和 v 是奇數，那末，假設

$$\frac{u+v}{2}=a,\quad \frac{u-v}{2}=b, \tag{98}$$

我們由等式

$$u=a+b,\quad v=a-b \tag{99}$$

決定數目 u 和 v．這兒 a 和 b 是不同奇偶的兩個整數．等式 (98)和 (99) 表明，任意一對互質的奇數 u 和 v 相應於一對互質的不同奇偶的數 a 和 b，而任意一對互質的不同奇偶的數 a 和 b 相應於一對互質的奇數 u 和 v．因此，在公式 (97) 中用 a 和 b 代替 u 和 v，我們得到所有的兩兩互質的三個正數 x,

y, z (x是奇數)，它們都是方程式(96)的解，而決定於公式

$$x=a^2-b^2,\quad y=2ab,\quad z=a^2+b^2, \tag{100}$$

這兒，a 和 b 在 $x>0$ 的條件下，是互質的兩個奇偶不同的整數。這個公式表明，x 和 y 是不同奇偶的數。若方程式(94)具有解 $[x_0, y_0, z_0]$，那就意味着，

$$[x_0^2]^2+[y_0^2]^2=z_0^2,$$

換句話說，三個數 (x_0^2, y_0^2, z_0) 就是方程式(96)的解。但在這種情況，應當存在着互質的奇偶不同的這樣兩個數 a 和 b，$a>b$，

$$x_0^2=a^2-b^2,\quad y_0^2=2ab,\quad z_0=a^2+b^2. \tag{101}$$

同時爲了明確，我們假定 x_0 是奇數而 y_0 是偶數。相反的假定，什麽也沒有改變，因爲用 x_0 代以 y_0，y_0 就代以 x_0。但我們已經知道〔參看等式(75)〕，一個奇數的平方被 4 除的時候，得到的餘數是 1。因而，從等式

$$x_0^2=a^2-b^2 \tag{102}$$

得到 a 是奇數而 b 是偶數。不是這樣的話，這個等式的左邊，在被 4 除的時候得出餘數 1，而右邊，因爲我們設 a 是偶數而 b 是奇數，餘數却是 -1。因爲 a 是奇數和 $(a,b)=1$，那末也就是 $(a,2b)=1$。但這樣一來，從等式

$$y_0^2=2ba$$

得到，

$$a=t^2,\quad 2b=s^2, \tag{103}$$

這兒 t 和 s 是某些整數。但從關係(102)得到，$[x_0, b, a]$ 是方

程式(96)的解．就是，

$$x_0=m^2-n^2,\quad b=2mn,\quad a=m^2+n^2,$$

這兒 m 和 n 是某些奇偶不同的互質數．從(103)的情況，

$$mn=\frac{b}{2}=(\frac{s}{2})^2,$$

由 m 和 n 是互質數的情況，得到

$$m=p^2,\quad n=q^2, \tag{104}$$

這兒 p 和 q 是異於零的整數．因為 $a=t^2$ 和 $a=m^2+n^2$，那末

$$q^4+p^4=t^2. \tag{105}$$

但

$$z_0=a^2+b^2>a^2.$$

因而

$$0<t=\sqrt{a}<\sqrt[4]{z_0}<z_0\quad (z_0>1). \tag{106}$$

設 $q=x_1$，$p=y_1$ 和 $t=z_1$，我們看出來，若存在解 $[x_0, y_0\ z_0]$，那末也必存在別的解 $[x_1, y_1, z_1]$，並且 $0<z_1<z_0$．這個求得方程式 (94) 的解的過程可以無限制地連續下去，我們於是得到一列的解

$$[x_0, y_0, z_0], [x_1, y_1, z_1], \cdots\cdots, [x_n, y_n, z_n,], \cdots\cdots,$$

並且正整數 $z_0, z_1, z_2, \cdots\cdots, z_n, \cdots\cdots$ 是單調遞降的；換句話說，對於它們，不等式

$$z_0>z_1>z_2>\cdots\cdots>z_n>\cdots\cdots$$

成立． 但正整數不可能組成一個單調遞降的無限數列，因為在這樣的數列中，不能夠多於 z_0 個項．這樣一來，若是假定方程式(94)至少有一組整數解 x, y, z，$xyz\neq 0$，我們就得到了一個矛盾．這就證明了，方程式(94)沒有正整數解，因而方程式

(93)也不具有正整數解$[x, y, z]$，因爲，在相反的情况中，若$[x,y,z]$是(93)的解，那末$[x,y,z^2]$就是(94)的解．

我們所使用的這種證明方法，叫做遞降法；它是借助於一組解，來做出有無限制遞降的正數z的無限多正整數解．對於一般情况的飛馬定理，代數環中的整數分解成同一環中的質因數的分解法的非唯一性，就阻止了這一方法的實施㊀．

我們注意，我們已經證明了，不只方程式(94)不存在整數解，而方程式

$$x^{4n}+y^{4n}=z^{2n}$$

也一樣不存在整數解．有趣的是方程式

$$x^4+y^2=z^2$$

具有無限多的正整數解，如$x=2$，$y=3$，$z=5$．這方程式的一切正整數解x,y,z的尋求，我們留給讀者．

再引一個用遞降法的例，其中思考過程多少有些改變．

〔範例〕 證明方程式

$$x^4+2y^4=z^2 \qquad (107)$$

不具有異於零的整數解x,y,z．假定方程式(107)具有正整數解$[x_0,y_0,z_0]$．我們立刻可以假定這些數是互質數，因爲假若它們具有最大公因數$d>1$，則$\frac{x_0}{d}$，$\frac{y_0}{d}$，$\frac{z_0}{d}$也是方程式(107)的解．它們中的兩個若有公因數存在，則它們三個也有公因數存在．此外，我們假定z_0是方程式(107)正整數解中一切可能有的z中最小的一個．因爲$[x_0,y_0,z_0]$是方程式(107)

㊀ 對於進一步的關於大飛馬定理的知識，我們推薦辛勤(A. Я. Хинчин)的'大飛馬定理'．

的解，所以 $[x_0^2, y_0^2, z_0^2]$ 是方程式

$$x^2+2y^2=z^2 \tag{108}$$

的解. 利用第 3 節的公式 (19')，它給出了 (108) 的一切正整數解，我們可以看出，存在着這樣的正整數 a 和 b，$(a,b)=1$，a 是奇數，而它們適合於等式

$$x_0^2=\pm(a^2-2b^2),\ y_0^2=2ab,\ z_0=a^2+2b^2. \tag{109}$$

從等式 $y_0^2=2ab$ 可得 b 必是偶數，因爲 y_0 是偶數，y_0^2 可以被 4 整除，而 a 是奇數. 因爲 $\frac{b}{2}$ 和 a 是互質數，由等式

$$\left(\frac{y_0}{2}\right)^2=a\cdot\frac{b}{2}$$

直接可得到，

$$a=m^2,\quad \frac{b}{2}=n^2,$$

這兒 m 和 n 是正整數，並且 $(m,2n)=1$. 但從(109)得

$$x_0^2=\pm(a^2-2b^2)=\pm\left[a^2-8\left(\frac{b}{2}\right)^2\right], \tag{110}$$

這兒 x_0 和 a 是奇數. 我們已經看到，一個奇數的平方，在被 4 除的時候得到的餘數是 1. 因此，(110)的左邊，在被 4 除的時候得到的餘數是 1，而 $a^2-8\left(\frac{b}{2}\right)^2$ 在被 4 除的時候得到的餘數也是 1. 這就是說，在等式(110)中，右邊括弧只能取正號. 現在等式(110)已經可以寫成這種形式

$$x_0^2=m^4-8n^4$$

或這種形式

$$x_0^2+2(2n^2)^2=(m^2)^2, \tag{111}$$

這兒 x_0，n 和 m 都是正整數，並且是互質數. 就是說，三個數 $x_0, 2n^2, m^2$ 是方程式(108)的解，並且 $x_0, 2n^2$ 和 m^2 是互質數.

因此，再由第3節公式(19′)，存在着這樣的整數 p 和 q，而 p 是奇數，$(p,q)=1$，

$$2n^2=2pq,\quad m^2=p^2+2q^2,\quad x_0=\pm(p^2-2q^2). \qquad (112)$$

但因爲 $(p,q)=1$ 和 $n^2=pq$，所以

$$p=s^2,\quad q=r^2;$$

這兒 s 和 r 是互質的整數．由此，最後得到關係

$$s^4+2r^4=m^2, \qquad (113)$$

它證明了數 s,r,m 組成方程式(107)的解．但從上面所得到的等式

$$z_0=a^2+2b^2,\quad a=m^2,$$

可得 $z_0>m$．由此，在有解 $[x_0,y_0,z_0]$ 以後，我們就求得另外的解 $[s,r,m]$，並且 $0<m<z_0$．這也跟我們所作的假定相矛盾；我們曾假定解 $[x_0,y_0,z_0]$ 具有的 z_0 是一切可能的 z 中的最小的一個．這樣一來，我們得到了一個矛盾，即不允許方程式(107)有解存在，並且證明了這個方程式不能有異於零的整數解．

我們現在留請讀者證明，方程式

$$x^4+4y^4=z^2,\qquad x^4-y^4=z^2,$$

$$x^4-y^4=2z^2,\qquad x^4-4y^4=z^2$$

不能有正整數解．

最後，我們來考察一下指數方程式．方程式

$$a^x+b^y=c^z, \qquad (114)$$

這兒 a,b 和 c 都是整數，並且不等於平方數和零．這方程式不能具有超過有限組數的正整數解 x,y,z．當 a,b 和 c 是任意代數數的時候，附帶不多的補充條件，這個論斷也有效，不特

如此，方程式

$$A\alpha_1^{x_1}\cdots\cdots\alpha_n^{x_n}+B\beta_1^{y_1}\cdots\cdots\beta_m^{y_m}+C\gamma_1^{z_1}\cdots\cdots\gamma_p^{z_p}=0, \quad (115)$$

這兒 A,B,C 是整數，$ABC\neq 0$，$\alpha_1,\cdots\cdots,\alpha_n$，$\beta_1,\cdots\cdots,\beta_m$，$\gamma_1,\cdots\cdots,\gamma_p$ 都是整數，並且三個數 α,β,γ，

$$\alpha=\alpha_1\cdots\cdots\alpha_n,\quad \beta=\beta_1\cdots\cdots\beta_m,\quad \gamma=\gamma_1\cdots\cdots\gamma_p,$$

是互質數，這個方程式只具有有限組數的整數解 $x_1,\cdots\cdots,x_n$，$y_1,\cdots\cdots,y_m$，$z_1,\cdots\cdots,z_p$。這個論斷也可以推廣到當 A,B,C 和 α_i，β_k，γ_s 是代數數的情形㊀。(115)型的方程式和它們的推廣顯示出很大的趣味，因為在代數數論中，證明了，每一個(81)型的代數數方程式對應着某些(115)型的指數方程式，並且(81)型方程式的每一組解對應於方程式(115)的整數解。這樣的對應還可以擴充到比(81)和(115)更一般型的方程式。

㊀ 參看前面引過的蓋里馮德的論文。